விழிப்(புடனிருந்திடுக)பாயிருந்திடுக



தமிழாக்கம்

முனைவர் ச.குப்பன்

விழிப்(புடனிருந்திடுக)பாயிருந்திடுக

முனைவர் ச. குப்பன்

FreeTamilEbooks.com

விழிப்(புடனிருந்திடுக)பாயிருந்திடுக

விழிப்(புடனிருந்திடுக)பாயிருந்திடுக

விழிப்(புடனிருந்திடுக)பாயிருந்திடுக

முனைவர் ச. குப்பன்

kuppansarkarai641@gmail.com

மின்னூல் வெளியீடு : FreeTamilEbooks.com

அட்டைப்படம் - லெனின் குருசாமி - guruleninn@gmail.com

மின்னூலாக்கம் - ஐஸ்வர்யா லெனின் - aishushanmugam09@gmail.com

This book was produced using pandoc

பதிவிறக்கம் செய்ய -
http://FreeTamilEbooks.com/ebooks/be_aware_and_beware

மின்னூல் வெளியீட்டாளர்: http://freetamilebooks.com

மெய்ப்புப் பார்ப்பு : விக்கிமூல பங்களிப்பார்கள்

அட்டைப்படம்: லெனின் குருசாமி - gurulenin@gmail.com

மின்னூலாக்கம்: ஐஸ்வர்யா லெனின் - aishushanmugam09@gmail.com

மின்னூலாக்க செயற்திட்டம்: கணியம் அறக்கட்டளை -
kaniyam.com/foundation

Ebook Publisher: http://freetamilebooks.com
Proof Reader : Wikisource Constributors
Cover Image: Lenin Gurusamy - gurulenin@gmail.com
Ebook Creation: Iswarya Lenin - aishushanmugam09@gmail.com
Ebook Project: Kaniyam Foundation - kaniyam.com/foundation

This Book was produced using LaTeX + Pandoc

முன்னுரை

சமீப ஆண்டுகளில் எண்ணிம(Digital) முறையில் பணம் செலுத்தும் பயன்பாட்டில் ஒரு எழுச்சி ஏற்பட்டுள்ளது. கோவிட்-19 தூண்டப்பட்ட பொதுமுடக்கங்களின் போது இது மேலும் வேகத்தை அதிகரித்தது. வாடிக்கையாளரின் வசதியை மேம்படுத்தும் அதே வேளையில், நிதி உள்ளடக்கத்தி**ன்(inclusion)** தேசிய நோக்கத்தையும் இது மேம்படுத்தியது. இருப்பினும், நிதி பரிமாற்றங்களைச் செய்வதற்கான வேகமும் எளிமையும் மேம்பட்டுள்ளதால், சில்லறை நிதிப் பரிமாற்றங்களில் புகாரளிக்கப்பட்ட மோசடிகளின் எண்ணிக்கையும் அதிகரித்துள்ளது. மோசடி செய்பவர்கள் பொதுமக்களின் கடின உழைப்பில் சம்பாதித்த பணத்தை, குறிப்பாக தொழில்நுட்ப-நிதிச்சூழல் அமைப்பைப் பற்றி முழுமையாகப் பரிச்சயமில்லாத எண்ணிம தளங்களைப் பயன்படுத்துவதில் புதிதாக நுழைபவர்களை ஏமாற்றுவதற்குப் புதுமையான வழிமுறைகளைப் பயன்படுத்துகின்றனர். இந்த கையேடு பல்வேறு மோசடி சம்பவங்களையும் **இந்திய நிதிகாப்பகவங்கியின்(RBI) குறைதீர்ப்பாளர்(Ombudsmen)** அலுவலகங்களில் பெறப்பட்ட புகார்களிலிருந்தும், குறிப்பாக எண்ணிம, மின்னணு ஆகிய நிதி பரிமாற்றங்களில் அனுபவமற்ற அல்லது அனுபவம்

இல்லாதவர்களுக்கு அதிகபட்ச நடைமுறை தகவல்களை வழங்குவதற்காக தொகுக்கப் பட்டுள்ளது. . நிதி பரிமாற்றங்களை மேற்கொள்ளும்போது எடுக்க வேண்டிய முன்னெச்சரிக்கை நடவடிக்கைகள் குறித்து தெரிவிக்கும் அதே வேளையில், மோசடி செய்பவர்கள் ஏமாற்றி, தவறாக வழிநடத்தும் வழிமுறைகள் குறித்தும் பொதுமக்களிடையே விழிப்புணர்வை ஏற்படுத்துவதற்காக இந்த சிறு புத்தகம் அமைந்துள்ளது. ஒருவரின் தனிப்பட்ட தகவல்களை, குறிப்பாக நிதித் தகவல்களை, எப்போதும் இரகசியமாக வைத்திருப்பது, அறியப்படாத அழைப்புகள் / மின்னஞ்சல்கள் / செய்திகள் குறித்து எச்சரிக்கையாக இருத்தல், நிதிப் பரிமாற்றங்களைச் செய்யும்போது கவனமாக இருத்தல், **பாதுகாப்பு சான்றுகளை** / கடவுச்சொற்களை அவ்வப்போது மாற்றியமைத்தல் ஆகியவற்றின் அவசியத்தை இது வலியுறுத்துகிறது. எனவே தலைப்பு **விழிப்(பாயிரு)புடனிரு (BE(A)WARE – Be Aware and Beware)!** இந்தக் கையேடு, இந்திய நிதிகாப்பகவங்கியின் நுகர்வோர் கல்வி, பாதுகாப்புத் துறையின் பொது விழிப்புணர்வு முயற்சியின் ஒரு பகுதியாகும், மேலும் இது மும்பை-II இன் குறைதீர்ப்பாளரின் அலுவலகத்தால் உருவாக்கப்பட்டுள்ளது.

விழிப்(புடன்)பாய் இருந்திடுவதற்கான செயல் முறைகளும் மோசடி பரிமாற்றங்களுக்கு எதிராக எடுக்க வேண்டிய முன்னெச்சரிக்கை நடவடிக்கைகளும் - வங்கிகள்

பகுதி-அ(Part-A) -வங்கிகள்



…

1.மோசடியான(Phishing) இணைப்புகள்



…

செயல் முறை(Modus Operandi)

• மோசடி செய்பவர்கள் மூன்றாம் தரப்பிலான மோசடி**(Phishing)** இணையதளத்தை உருவாக்குகிறார்கள், இது ஏற்கனவே உள்ள உண்மையான இணையதளத்தைப் போன்றே தோற்றமளிக்கிறது - இவை வங்கியின் இணையதளம் அல்லது மின்-வணிக இணையதளம் அல்லது தேடுபொறி போன்றவைகளாகும்.

• இந்த இணையதளங்களுக்கான இணைப்புகள் குறுந்தகவல் சேவை (Short Message Service (SMS)) / சமூக ஊடகங்கள் / மின்னஞ்சல் / உடனடி

செய்தியாளர் போன்றவற்றின் மூலம் மோசடி செய்பவர்களால் பரப்பப்படுகின்றன

. • பல வாடிக்கையாளர்கள் விரிவான ஒரேசீரானவளஇடங்காட்டியை (Uniform Resource Locator (URL)) சரிபார்க்காமல் இணைப்பை சொடுக்குதல் செய்து, தனிப்பட்ட அடையாள எண் (Personal Identification Number (PIN)), ஒரு முறை மட்டுமானகடவுச்சொல் (One Time Password (OTP)), கடவுச்சொல் (Password) போன்ற பயனாளர்உள்ளிடுகின்ற பாதுகாப்பான சான்றுகள் . மோசடி செய்பவர்களால் கைப்பற்றப்பட்டு பயன்படுத்தப்படுகின்றன

முன்னெச்சரிக்கை நடவடிக்கைகள்

• அறியப்படாத / சரிபார்க்கப்படாத இணைப்புகளை சொடுக்குதல் செய்திடாதீர்கள் எதிர்காலத்தில் தவறுதலாக அவற்றை அணுகுவதைத் தவிர்க்க, தெரியாத அனுப்புநர் அனுப்பிய குறுந்தகவலை (SMS) / மின்னஞ்சலை உடனடியாக நீக்கிடுக.

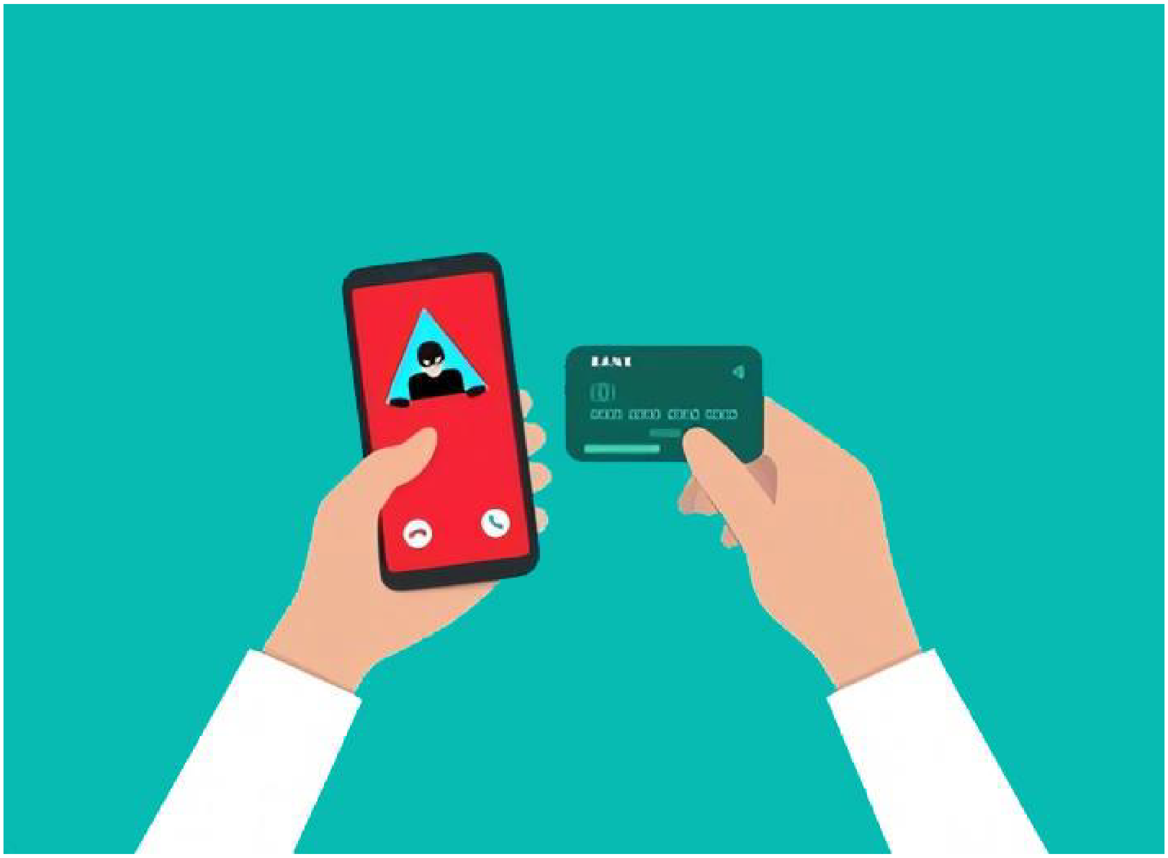
• வங்கி / மின்-வணிகம் / தேடுபொறி இணையதளத்திற்கான இணைப்புகளை வழங்கும் குழுவிலிருந்து விலகிடுக அத்தகைய மின்னஞ்சல்களை நீக்கும் முன் அனுப்புநரின் மின்னஞ்சல் சுட்டியைத் தடுத்திடுக.

• எப்போதும் வங்கியின் / சேவை வழங்குநரின் அதிகாரப்பூர்வ இணையதளத்திற்கு மட்டும் செல்க. குறிப்பாக நிதிச் சான்றுகளை உள்ளிட

வேண்டிய இணையதள விவரங்களைக் கவனமாகச் சரிபார்த்திடுக. பாதுகாப்பிற்கானசான்றிதழ்களை உள்ளிடுவதற்கு முன் இணையதளத்தில் பாதுகாப்பான அடையாளத்தை (பூட்டு சின்னத்துடன் கூடிய https) உள்ளதா எனச் சரிபார்த்திடுக.

• எழுத்துப் பிழைகளுக்கு மின்னஞ்சல்களில் பெறப்பட்ட இணையதள முகவரிகளையும்(URL) களப்பெயர்களையும் சரிபார்த்திடுக. சந்தேகம் இருந்தால் உடனடியாக அதுகுறித்து தகவல்தெரிவித்திடுக

2.முறைகேடான(Vishing) அழைப்புகள்



…

செயல் முறை

• வஞ்சகர்கள் தொலைபேசி அழைப்பு / சமூக ஊடகங்கள் மூலம் வங்கியாளர்கள் / நிறுவன நிர்வாகிகள் / காப்பீட்டு முகவர்கள் / அரசு அதிகாரிகள் போன்ற தோற்றத்தில் வாடிக்கையாளர்களை அழைக்கி றார்கள் அல்லது அணுகுகிறார்கள். நம்பிக்கையைப் பெற, ஏமாற்றுக் காரர்கள் வாடிக்கையாளரின் சரியானபெயர் அல்லது பிறந்த தேதி போன்ற சில வாடிக்கையாளர் விவரங்களைப் பகிர்ந்து கொள்கிறார்கள்.

• சில சந்தர்ப்பங்களில், அனுமதியில்லாத நிதி நடவடிக்கைகளை தடுத்துநிறுத்திடவேண்டி ,அவைகளுக்கு அபராதங்களை நிறுத்தி வைத்தல், கவர்ச்சிகரமான தள்ளுபடிஅளித்தல் போன்றவற்றை அவசரமாக/ உடனடியாக செய்யவேண்டியுள்ளதால் கடவுச்சொற்கள் / OTP / PIN / அட்டை சரிபார்ப்பு மதிப்பு (Card Verification Value (CVV)) போன்ற இரகசிய விவரங்களைப் உடனடியாக பகிர்ந்திடுமாறு ஏமாற்றுபவர்கள் வாடிக்கையாளர்களை நெருக்குதல்தந்து / ஏமாற்றி.. இவைகளை வாடிக்கையாளர்களிடமிருந்து பெற்ற பின்னர் இதனை மோசடியாகப் பயன்படுத்தி தஙகளுடைய அபகரிப்புபணியை மேற்கொள்கின்றனர்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• வங்கி அதிகாரிகள் / நிதி நிறுவனங்கள் / இந்திய சேமநல வங்கி(RBI) / எந்தவொரு உண்மையான நிறுவனமும் பயனர் பெயர் / கடவுச்சொல் / அட்டை விவரங்கள் / CVV / OTP போன்ற இரகசியத் தகவல்களைப் பகிர்ந்து கொள்ளுமாறு வாடிக்கையாளர்களிடம் எப்போதும் கோருவதில்லை.

• இந்த இரகசிய விவரங்களை யாருடனும், உங்கள் சொந்த குடும்ப உறுப்பினர்களுடனும் நண்பர்களுடனும்கூடபகிர்ந்து கொள்ள வேண்டாம்.

3.நேரடிஇணைய விற்பனை தளங்கள் பயன்படுத்திடும் மோசடிகள்



...

செயல் முறை

• மோசடி செய்பவர்கள் நேரடிஇணைய விற்பனை தளங்களில் வாங்குபவர்கள் போல் நடித்து விற்பனையாளரின் பொருட்கள் மீது ஆர்வம் காட்டுகின்றனர். பல மோசடி செய்பவர்கள் தன்னம்பிக்கையைப் பெறுவதற்காக தொலைதூர இடங்களில் பாதுகாப்புப் பணியாளர்களாக நடிக்கின்றனர்.

• விற்பனையாளருக்கு பணம் செலுத்துவதற்குப் பதிலாக, அவர்கள் ஒரேசீரானகொடுப்பனவுகளின்இடைமுகம் (Unified Payments Interface (UPI)) எனும் பயன்பாட்டின் மூலம் "பணம் கோருதல்(request money)"

எனும் வாய்ப்பினைப் பயன்படுத்துகின்றனர் UPI இன் சுட்டிஎண்ணை(PIN) உள்ளிட்டு விற்பனையாளர் கோரிக்கையை அங்கீகரிக்க வேண்டும் என்று வலியுறுத்துகின்றனர். விற்பனையாளர் சுட்டிஎண்ணை உள்ளிட்டதும், மோசடி செய்பவரின் கணக்கிற்கு பணத்தினை மாற்றிகொள்கின்றனர்

முன்னெச்சரிக்கை நடவடிக்கைகள்

• நேரடிஇணைய விற்பனை தளங்களைப் பயன்படுத்தி பொருட்களை வாங்கும்போது அல்லது விற்கும்போது எப்போதும் கவனமாக இருந்திடுக.

• பணத்தைப் பெற எங்கும் (PIN) / கடவுச்சொல்லை உள்ளிடவேண்டிய அவசியமில்லை என்பதை எப்போதும் நினைவில் கொள்க.

• ஒரு பரிமாற்றத்தினை முடிக்க UPI அல்லது வேறு ஏதேனும் பயன் பாட்டிற்கு சுட்டிஎண்ணை(PIN) உள்ளிட வேண்டுமெனில், அதைப் நாம் பெறுவதற்குப் பதிலாக நாம் நம்முடைய பணத்தை மற்றவர்களுக்கு அனுப்ப உதவுகின்றோம் என்பதே பொருளாகும் என்ற செய்தியை மனதில் கொள்க.

4.அறியப்படாத / சரிபார்க்கப்படாத கைபேசி பயன்பாடுகளைப் பயன்படுத்துவதால் ஏற்படும் மோசடிகள்



…

செயல் முறை

• மோசடி செய்பவர்கள் குறுந்தகவல் / மின்னஞ்சல் / சமூக ஊடகம் / உடனடி செய்தியாளர் போன்றவற்றின் மூலம் தகவல்களை பரப்பு கிறார்கள், சில பயன்பாடுகளின்(apps)இணைப்புகள், அங்கீகரிக்கப்பட்ட நிறுவனங்களின் தற்போதைய பயன்பாடுகளைப் போன்றே தோன்றும்.

• மோசடி செய்பவர்கள் வாடிக்கையாளரின் கைபேசி / மடிக்கணினி / மேசைக்கணினி போன்றவற்றில் அறியப்படாத / சரிபார்க்கப்படாத பயன்பாடுகளை பதிவிறக்கம் செய்வதன் மூலம் அத்தகைய

இணைப்புகளைசொடுக்குதலைசெய்திடுமாறு வாடிக்கையாளரை ஏமாற்றுகிறார்கள்.

• தீங்கிழைக்கும் பயன்பாட்டினை பதிவிறக்கம் செய்யப்பட்டவுடன், மோசடி செய்பவர் வாடிக்கையாளரின் சாதனத்திற்கான முழுமையான அணுகலைப் பெறுகிறார். சாதனத்தில் சேமிக்கப்பட்ட இரகசிய விவரங்கள், அத்தகைய பயன்பாடுகளை நிறுவுவதற்கு முன்னர் / பின்னர் பெறப்பட்ட செய்திகள் / OTPs ஆகியவை இதில் அடங்கும்

முன்னெச்சரிக்கை நடவடிக்கைகள்

• சரிபார்க்கப்படாத/தெரியாத ஆதாரங்களில் இருந்தும் அல்லது அறியப்படாத நபரால் கேட்கப்படும்/வழிகாட்டப்படும்போதும் பயன்பாட்டினை பதிவிறக்கம் செய்யாதீர்கள்.

• பதிவிறக்கம் செய்வதற்கு முன் ஒரு விவேகமான நடைமுறையாக, பதிவிறக்கம் செய்யப்படும் பயன்பாட்டின் வெளியீட்டாளர்கள் / உரிமையாளர்கள் , அதன் பயனர் மதிப்பீடுகள் போன்றவற்றைச் சரிபார்த்திடுக.

• பயன்பாட்டைப் பதிவிறக்கும் போது, அனுமதி/கள், அது தேடும் தொடர்புகள், புகைப்படங்கள் போன்ற உங்கள் தரவுக்கான அணுகலைச் சரிபார்த்திடுக. விரும்பிய பயன்பாட்டைப் பயன்படுத்துவதற்கு முற்றிலும் தேவைப்படும் அனுமதிகளை மட்டும் கொடுத்திடுக.

5.தயார்நிலைகாசாளர்(ATM) அட்டையின் தரவை கவணித்தல் (skimming)



…

செயல் முறை

• மோசடி செய்பவர்கள் **ATM** இயந்திரங்களில் **தரவை கவணித்தல் (skimming)** எனும் சாதனங்களை நிறுவுகைசெய்து, வாடிக்கையாளரின் அட்டையிலிருந்து தரவைத் திருடுகிறார்கள்.

• மோசடி செய்பவர்கள் ஒரு போலியான விசைப்பலகை அல்லது ஒருசிறிய/ குண்டூசிஅளவேயானபடபிடிப்புகருவியை நிறுவுகை செய்திருக் கலாம்,உடன்**ATMஇன்** சுட்டிஎண்ணை(PIN) தெரிந்துகொள்ள

முனையும் இது நம்முடைய சாதாரண பார்வையிலிருந்து நன்கு மறைவாகஇருக்கும்.

• சில சமயங்களில், **ATM** இயந்திரத்தில் வாடிக்கையாளர் சுட்டி எண்ணை(PIN) உள்ளிடும்போது, அருகில் நிற்கும் மற்ற வாடிக்கை யாளரைப் போல் நடித்து மோசடி செய்பவர்கள், சுட்டிஎண்ணை(PIN) தெரிந்துகொள்ள அணுகுவார்கள்.

• இந்தத் தரவினைகொண்டு நகல் அட்டையை உருவாக்கவும் வாடிக்கையாளரின் கணக்கிலிருந்து பணத்தை எடுக்கவும் பயன்படுத்தி கொள்வார்கள்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• பரிமாற்றம் செய்வதற்கு முன், சுட்டிஎண்ணை(PIN) இயந்திரத்தின் அட்டையை செருகும் செருகுவாய்க்கு அல்லது விசைப்பலகைக்கு அருகில் கூடுதல் சாதனம் எதுவும் இணைக்கப்படவில்லை என்பதை எப்போதும் சரிபார்த்திடுக

. • சுட்டிஎண்ணை(PIN) உள்ளிடும் போது உங்களின் மற்றொரு கையால் விசைப்பலகையை மூடிபாதுகாத்திடுக.

• **ATM** அட்டையில் சுட்டிஎண்ணை(PIN)எழுதிவைத்திட வேண்டாம்.

• அருகில் நிற்கும் வேறுஅறியாத / தெரியாத நபரின் முன்னிலையில் **ATM** இயந்திரத்தில் அட்டையின்சுட்டிஎண்ணை(PIN) உள்ளிட வேண்டாம்.

• **ATM** இயந்திரத்திலிருந்து பணம் எடுப்பதற்காக உங்களுடைய **ATM** அட்டையை வேறு யாரிடமும் கொடுக்க வேண்டாம்.

• **ATMஇயந்திரங்**களில் அறியாத /தெரியாத நபர்கள் வழங்கிய வழிமுறைகளைப் பின்பற்றாதீர்கள் அல்லது அந்நியர்களிடமிருந்து/ தெரியாத நபர்களிடமிருந்து உதவி / வழிகாட்டுதலைப் பெறாதீர்கள்.

• **ATMஇயந்திரங்**கள் பணம் வழங்காவிட்டால், **ATM இயந்திரங்**களி லிருந்து வெளியேறும் முன் ‘Cancel’ எனும் பொத்தானை அழுத்தி வழக்கமானமுகப்புத் திரைதோன்றும் வரை காத்திருக்கவும்.

6.திரைப்பகிர்வு பயன்பாடு / தொலைநிலை அணுகல் பயன்படுத்திடும் மோசடிகள்



...

செயல் முறை

• மோசடி செய்பவர்கள் வாடிக்கையாளரை ஏமாற்றி திரைப் பகிர்வு பயன்பாட்டைப் பதிவிறக்கம்செய்திடுமாறு கோருகின்றனர்.

• அத்தகைய பயன்பாட்டைப் பயன்படுத்தி, மோசடி செய்பவர்கள் வாடிக்கையாளரின் கைபேசி / மடிக்கணினியைப் பார்வையிடலாம் / கட்டுப்படுத்தலாம் , வாடிக்கையாளரின் நிதிச் சான்றுகளுக்கான அணுகலைப் பெறலாம்.

• மோசடி செய்பவர்கள் இந்த தகவலை அங்கீகரிக்கப்படாத நிதி பரிமாற்றத்தை மேற்கொள்கின்றனர் அல்லது வாடிக்கையாளரின் இணைய

வங்கி / கொடுப்பனவு பயன்பாடுகளைப் பயன்படுத்தி பணம் எடுத்துகொள்கின்றனர்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• உங்கள் சாதனம் ஏதேனும் தொழில்நுட்பக் கோளாறை எதிர்கொண்டால், நீங்கள் ஏதேனும் திரைப் பகிர்வு பயன்பாட்டைப் பதிவிறக்க வேண்டும் எனில், உங்கள் சாதனத்திலிருந்து பணம் செலுத்துதல் தொடர்பான அனைத்துப் பயன்பாடுகளையும் செயலிழக்கச் செய்திடுக / வெளியேறிடுக.

• நிறுவனத்தின் அதிகாரப்பூர்வ இணையதளத்தில் தோன்றும் அதிகாரப்பூர்வ கட்டணமில்லா எண் மூலம் உங்களுக்கு அறிவுறுத்தப் படும் போது மட்டுமே அத்தகைய பயன்பாடுகளைப் பதிவிறக்கம் செய்திடுக. நிறுவனத்தின் நிர்வாகி ஒருவர் தனது தனிப்பட்ட தொடர்பு எண் மூலம் உங்களைத் தொடர்பு கொண்டால், அத்தகைய பயன்பாடுகளைப் பதிவிறக்கம் செய்திட வேண்டாம்.

• அந்தபணி முடிந்தவுடன், உங்கள் சாதனத்திலிருந்து திரைப் பகிர்வு பயன்பாடு அகற்றப்பட்டதை உறுதிசெய்திடுக.

7.சந்தாதாரர் அடையாள கூறினை(SIM) மாற்றிடுதல்(swap) / சந்தாதாரர் அடையாள கூறினை(SIM)போலியாகச்செய்தல்(cloning)



…

செயல் முறை

• மோசடி செய்பவர்கள் வாடிக்கையாளரின் சந்தாதாரர் அடையாள கூறின் (Subscriber Identity Module (SIM)) அட்டைக்கான அணுகலைப் பெறுவார்கள் அல்லது வாடிக்கையாளரின் வங்கிக் கணக்கில் இணைக்கப்பட்ட பதிவு செய்யப்பட்ட கைபேசி எண்ணுக்கு நகல் SIMஅட்டை (மின்னனுSIM உட்பட) பெறமுயற்சிக்கலாம்.

• மோசடி செய்பவர்கள் அத்தகைய மேசடி SIMஇல் பெறப்பட்ட OTP ஐ அங்கீகரிக்கப்படாத பரிமாற்றங்களை மேற்கொள்ள பயன்படுத்துகின்றனர்.

• மோசடி செய்பவர்கள் பொதுவாக வாடிக்கையாளரிடமிருந்து தனிப்பட்ட/ அடையாள விவரங்களை தொலைபேசி/கைபேசி வலைபின்னல் ஊழியர்களாகக் காட்டிக் கொண்டு, -3G(4G) இலிருந்து 4G(5G) க்கு SIM அட்டையை இலவசமாக மேம்படுத்துதல் அல்லது கூடுதல் பலன்களை வழங்குதல் போன்ற சலுகைகளின் பெயரில் வாடிக்கையாளர் விவரங்களைக் கோருகின்றனர்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• உங்களுடைய SIMஅட்டை தொடர்பான அடையாளச் சான்றுகளை யாரிடமும் ஒருபோதும் பகிர்ந்துகொள்ள வேண்டாம்.

• உங்கள் கைபேசியில் கைபேசிவலையின்பின்னல் அணுகல் குறித்து கவனமாக இருந்திடுக. வழக்கமான சூழலில் கணிசமான நேரம் உங்கள் கைபேசியில் கைபேசியின் வலைபின்னல்இணைப்பு இல்லை என்றால், உடனடியாக கைபேசி இயக்குபவரைத் தொடர்புகொண்டு உங்கள்

கைபேசி எண்ணுக்கு நகல் SIMஅட்டை எதுவும் யாருக்கும்வழங்கப்படவில்லை என்பதை உறுதிப்படுத்திகொள்க.

8.தேடுபொறிகளின் மூலமான கிடைத்திடும்முடிவுகளில் அறிமுக ஆவணத்தினை ஒத்திசைவு செய்வதன் மூலமான மோசடிகள்



…

செயல் முறை

• வாடிக்கையாளர்கள் தங்கள் வங்கி, காப்பீட்டு நிறுவனம், ஆதார் புதுப்பிப்பு மையம் போன்றவற்றின் தொடர்பு விவரங்கள் / வாடிக்கையாளர் பராமரிப்பு எண்களைப் பெற தேடுபொறிகளைப் பயன்படுத்துகின்றனர். தேடுபொறிகளில் உள்ள இந்தத் தொடர்பு

விவரங்கள் பெரும்பாலும் அந்தந்த நிறுவனத்தைச் சேர்ந்தவை அல்ல, ஆனால் மோசடி செய்பவர்களால் அவைஅவ்வாறு தோன்றும்.

• தேடுபொறியில் வங்கியின் / நிறுவனத்தின் தொடர்பு எண்களாகக் காட்டப்படும் மோசடி செய்பவர்களின் அறியப்படாத / சரிபார்க்கப்படாத தொடர்பு எண்களை வாடிக்கையாளர்கள் தொடர்பு கொள்ளலாம்.

• வாடிக்கையாளர்கள் இந்தத் தொடர்பு எண்களை அழைத்தவுடன், மோசடி செய்பவர்கள் வாடிக்கையாளர்களிடம் தங்கள் அட்டைச் சான்றுகள் / விவரங்களைச் சரிபார்ப்பதற்காகப் பகிர்ந்து கொள்ளச் கோருகிறார்கள்.

• மோசடி செய்பவர் **RE** இன் உண்மையான பிரதிநிதியாக இருப்பதாகக் கருதி, வாடிக்கையாளர்கள் தங்கள் பாதுகாப்பு விவரங்களைப் பகிர்ந்து கொள்கிறார்கள், இதனால் மோசடிகளுக்கு இரையாகிறார்கள்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• வங்கிகளின் / நிறுவனங்களின் அதிகாரப்பூர்வ இணையதளங்களில் இருந்து வாடிக்கையாளர் பராமரிப்பு தொடர்பு விவரங்களை எப்போதும் பெற்றிடுக.

• தேடுபொறி முடிவுகளின் பக்கத்தில் காட்டப்படும் எண்களை நேரடியாக அழைக்க வேண்டாம், ஏனெனில் இவை பெரும்பாலும் மோசடி செய்பவர்களால் மறைக்கப்படுகின்றன.

• வாடிக்கையாளர் பாதுகாப்பு எண்களானவை ஒருபோதும் கைபேசி எண்களின் வடிவத்தில் இல்லை என்பதையும் நினைவில் கொள்க

9.QR குறியீடு வருடிதல் மூலமான மோசடி



…

செயல் முறை

• மோசடி செய்பவர்கள் அடிக்கடி வாடிக்கையாளர்களை பல்வேறு சாக்குப்போக்குகளின் கீழ் தொடர்பு கொண்டு வாடிக்கையாளர்களின் கைபேசியில் உள்ள பயன்பாடுகளைப் பயன்படுத்தி விரைவான பதில்செயல் (QR) குறியீடுகளை வருடுதல் செய்வதில் ஏமாற்றுகின்றனர்.

• அத்தகைய QR குறியீடுகளை வருடுதல் செய்வதன் மூலம், வாடிக்கையாளர்கள் தங்கள் கணக்கில் இருந்து பணத்தை எடுக்க மோசடி செய்பவர்களை அறியாமலேயே அங்கீகரிக்கலாம்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• எந்தவொரு கட்டண பயன்பாட்டையும் பயன்படுத்தி QR குறியீடு/களை வருடுதல் செய்திடும் போது கவனமாக இருந்திடுக. QR குறியீடுகளில் குறிப்பிட்ட கணக்கிற்குப் பணத்தை மாற்றுவதற்கு கணக்கு விவரங்கள் பதிக்கப்பட்டிருக்கும்.

• பணத்தைப் பெற எந்த QR குறியீட்டையும் வருடுதல் செய்திட வேண்டாம். பணம்பெற்றுகொண்டதுதொடர்பான பணப் பரிமாற்றங்களுக்கு பட்டைக்குறியீடுகள் / QR குறியீடுகளை வருடுதல் செய்வது அல்லது கைபேசிவங்கிசுட்டிஎண் (m-PIN), கடவுச்சொற்கள் போன்றவற்றை உள்ளிடுவது தேவையில்லை.

10.சமூக ஊடகங்களில்(social media) ஆள்மாறாட்டம்



…

செயல் முறை

• மோசடி செய்பவர்கள் பேஸ்புக், இன்ஸ்டாகிராம், ட்விட்டர் போன்ற சமூக ஊடக தளங்களைப் பயன்படுத்துபவர்களின் விவரங்களைப் பயன்படுத்தி போலியான கணக்குகளை உருவாக்குகிறார்கள்.

• மோசடி செய்பவர்கள் பயனர்களின் நண்பர்களுக்கு அவசர மருத்துவ உதவிகள், கடனைதிருப்புதல்கள் போன்றவற்றிற்காக பணம்கேட்டு ஒரு கோரிக்கையை அனுப்புகிறார்கள்.

• மோசடி செய்பவர்கள், போலி விவரங்களைப் பயன்படுத்தி, பயனர்களைத் தொடர்புகொண்டு, குறிப்பிட்ட காலத்திற்கு பயனாளர்களின் நம்பிக்கையைப் பெறவும். பயனாளர்கள் தங்கள் தனிப்பட்ட அல்லது

தனிப்பட்ட தகவல்களைப் பகிரும் போது, மோசடி செய்பவர்கள் பயனாளர்களை அச்சுறுத்தவோ அல்லது மிரட்டி பணம் பறிக்கவோ அத்தகைய தகவல்களைப் பயன்படுத்திகொள்கின்றனர்.

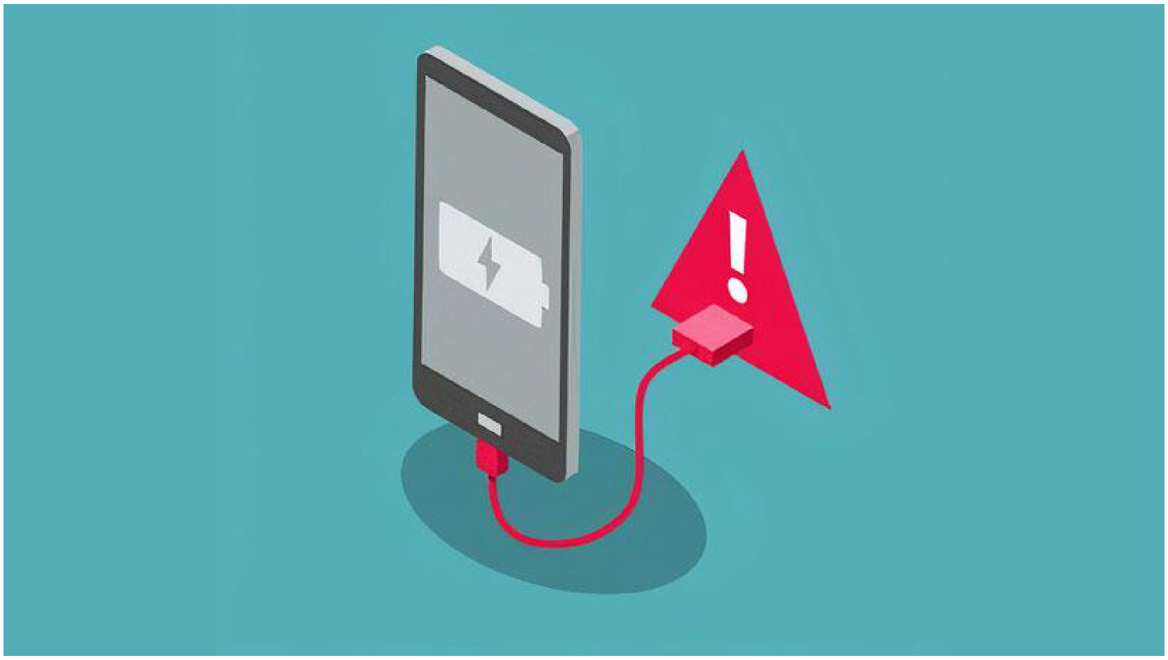
முன்னெச்சரிக்கை நடவடிக்கைகள்

• சுயவிவரம் ஆள்மாறாட்டம் செய்யப்படவில்லை என்பதை உறுதிப்படுத்த, தொலைபேசி அழைப்பு / நேரடி சந்திப்பு மூலம் உறுதிப்படுத்துவதன் மூலம், நண்பர் / உறவினரின் நிதிக் கோரிக்கையின் உண்மையான தன்மையை எப்போதும் சரிபார்த்திடுக.

• தெரியாதநபர்களுக்கு இணையத்தின்மூலம் பணம்செலுத்த வேண்டாம்.

• தனிப்பட்ட இரகசிய தகவல்களை சமூக ஊடக தளங்களில் பகிர்ந்து கொள்ள வேண்டாம்.

11.பழச்சாறாக அபகரித்தல்(Juice jacking)



…

செயல் முறை

• கைபேசி மின்னேற்றவாயில், கோப்புகள் / தரவை மாற்றிடவும் பயன்படுத்திகொள்ளலாம்.

• மோசடி செய்பவர்கள் கைபேசிக்கான பொது மின்னேற்றவாயில்களைப் பயன்படுத்தி நச்சுநிரலை(malware) அங்கு இணைக்கப்பட்ட வாடிக்கையாளர் கைபேசிகளுக்கு மாற்றுகிறார்கள், வாடிக்கையாளர்களின் கைபேசிகளில் இருந்து மின்னஞ்சல்கள், குறுஞ்செய்திகளில், சேமித்த கடவுச்சொற்கள் போன்ற முக்கியமான தரவினைக் கட்டுப்படுத்த / அணுக / பழச்சாறாக அபகரித்திடுகிறார்கள் (**(Juice jacking)**).

முன்னெச்சரிக்கை நடவடிக்கைகள்

• பொதுவான தெரியாத/ அறியப்படாத கைபேசிமின்னேற்றவாயில்கள் / கம்பிகளைப் பயன்படுத்துவதைஅறவேத் தவிர்த்திடுக

12.பரிசுசீட்டு மோசடி



...

செயல் முறை

• மோசடி செய்பவர்கள் குறிப்பிட்டதொரு வாடிக்கையாளர் மிகப்பெரிய பரிசினை வென்றதாக மின்னஞ்சல்களை அனுப்புகின்றனர் அல்லது தொலைபேசி அழைப்புகளை மேற்கொள்கின்றனர். எவ்வாறாயினும், பணத்தைப் பெறுவதற்காக, மோசடி செய்பவர்கள் வாடிக்கையாளர்கள்

தங்கள் வங்கிக் கணக்கு / கடனட்டை விவரங்களை மோசடி செய்பவர்களால் கைப்பற்றப்பட்ட இணையதளத்தில் உள்ளிடுவதன் மூலம் அவர்களின் அடையாளத்தை உறுதிப்படுத்துமாறு கேட்டுக் கொள்கிறார்கள்.

• மோசடி செய்பவர்கள் பரிசுத்தொகையைப்/பொருளைப் பெறுவதற்கு வாடிக்கையாளர்களை வரி/அந்நிய செலாவணி கட்டணங்கள்/ முன்கூட்டியேயான செலவிணங்கள் அல்லது கொண்டுவரும் கட்டணம், செயலாக்க கட்டணம்/ கையாளுதல் கட்டணம் போன்றவற்றை உடனடியாகச் செலுத்த வேண்டுமாறு கோருகின்றனர்.

• சில சந்தர்ப்பங்களில் மோசடி செய்பவர்கள், இந்திய சேமநலவங்கி (RBI)அல்லது ஒரு வெளிநாட்டு வங்கி / நிறுவனம் / சர்வதேச நிதி நிறுவனத்தின் பிரதிநிதியாகக் காட்டிக்கொண்டு, அந்த நிறுவனத்திட மிருந்து அதிக தொகையை வெளிநாட்டு நாணயமாகப் பெறுவதற்கு ஒப்பீட்டளவில் சிறிய தொகையை மட்டும்மாற்றிடுமாறு வாடிக்கை யாளரிடம் கோரலாம்.

• கோரப்பட்ட பணம் பொதுவாக வாக்குறுதியளிக்கப்பட்டபரிசுசீட்டில் / பரிசில் மிகச் சிறிய சதவீதமாக இருப்பதால், வாடிக்கையாளர் மோசடி செய்பவரின் வலையில் விழுந்து பணம் செலுத்தநேரிடலாம்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• இது போன்ற நம்பமுடியாத பரிசு அல்லது சலுகைகள் குறித்து **விழிப்பாகஇருந்திடுக** - யாரும் குறிப்பாக இவ்வளவு பெரிய தொகையை இலவசமாக பணம் கொடுப்பதில்லை,

• எந்தபரிசுசீட்டு அழைப்புகளுக்குப்/ மின்னஞ்சல்களுக்குப் பதில் பணம் செலுத்தவோ அல்லது பாதுகாப்பிற்கான சான்றிதழ்களை பகிர்ந்து கொள்ளவோ வேண்டாம்.

• இந்திய சேமநல வங்கியானது(RBI) ஒருபோதும் பொதுமக்களுக்கான கணக்குகளை நேரடியாக துவங்குவதில்லை அல்லது அவர்களிடமிருந்து வைப்புத்தொகையைப் பெறுவதில்லை. இத்தகைய செய்திகள் மோசடியானவை.

• இந்திய சேமநல வங்கியானது(RBI) பொதுமக்களின் தனிப்பட்ட / வங்கி விவரங்களை ஒருபோதும் கோருவதில்லை. போலியான இந்திய சேமநல வங்கி (RBI)வணிகமுத்திரை**களையும்** செய்திகளையும் குறித்து **விழிப்பாயிருந்திடுக**.

• பரிசுத் தொகைகள், அரசாங்க உதவித்தொகைகள் ஆகியவற்றினைப் பெற உங்கள் வாடிக்கையாளரை அறிந்து கொள்ளுங்கள் (KYC) புதுப்பிப்புகளை வழங்கும்/ உறுதியளிக்கும் செய்திகளுக்கு ஒருபோதும் பதிலளிக்க வேண்டாம்.

13.போலியாகவேலைதரும் இணையதள மோசடி



…

செயல் முறை

• மோசடி செய்பவர்கள் போலியான வேலை தேடல் இணையதளங்களை உருவாக்கி, வேலை தேடுபவர்கள் தங்கள் வங்கிக் கணக்கு / கடனட்டை / பற்ற**ட்டை** ஆகியவற்றின் பாதுகாப்பு சான்றுகளை பதிவு செய்யும் போது இந்த இணையதளங்களில் பகிர்ந்து கொள்ளும்போது, அவர்களது கணக்குகள் பாதிக்கப்படும்.

• மோசடி செய்பவர்கள் புகழ்பெற்ற நிறுவனங்களின் அதிகாரிகளாகக் காட்டிக் கொண்டு, போலியான நேர்காணல்களை நடத்தி வேலை வழங்கு கிறார்கள். வேலை தேடுபவர் பதிவுகட்டணம், கட்டாயப் பயிற்சி

கட்டணம், மடிக்கணினி போன்றவற்றிற்கான நிதியை பரிமாற்றத் தூண்டப்படுகிறார்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• வெளிநாட்டு நிறுவனங்கள் உட்பட எந்தவொரு வேலை வாய்ப்பிற்கும், முதலில் பணியமர்த்தும் நிறுவனம் / அதன் பிரதிநிதியின் அடையாள விவரங்களையும், தொடர்பு விவரங்களையும் உறுதிப்படுத்திடுக.

• வேலை வழங்கும் ஒரு உண்மையான நிறுவனம், வேலையை வழங்குவதற்கு ஒருபோதும் பணம் கோராது என்பதை எப்போதும் நினைவில் கொள்க.

• தெரியாத வேலை தேடும் இணையதளங்களில் பணம் செலுத்த வேண்டாம்.

14.பணக் கழுதைகள் (Money Mules)



…

செயல் முறை

• பணக்கழுதை(Money Mule) என்பது, தங்கள் வங்கிக் கணக்கு/கள் மூலம் திருடப்பட்ட/ சட்டவிரோதமான பணத்தை மோசடி செய்பவர்களால் ஏமாற்றப்பட்ட அப்பாவியாக பாதிக்கப்பட்டவர்களை விவரிக்கப் பயன்படும் சொல்லாகும்.

• மோசடி செய்பவர்கள் மின்னஞ்சல்கள், சமூக ஊடகங்கள் போன்ற வற்றின் மூலம் வாடிக்கையாளர்களைத் தொடர்புகொண்டு, கவர்ச்சி கரமான கழிவுத்தொகைகளுக்கு ஈடாக, அவர்களின் (பணக் கழுதை) வங்கிக் கணக்குகளில் பணத்தைப் பெறும்படி அவர்களை நம்பவைக்கி றார்கள்.

• பணக் கழுதை மற்றொரு பணக் கழுதையின் கணக்கிற்குப் பணத்தைப் பரிமாற்றம் செய்யும்படி, ஒரு சங்கிலியைத் தொடங்கி, இறுதியில் பணமோசடி செய்பவரின் கணக்கிற்கு மாற்றப்படும்.

• மாற்றாக, மோசடி செய்பவர் பணத்தை எடுத்து ஒருவரிடம் ஒப்படைக்குமாறு பணக் கழுதையை வழிநடத்தலாம்.

• இத்தகைய மோசடிகள் புகாரளிக்கப்பட்டால், பணக் கழுதையானது பணமோசடி செய்த தற்கான காவல்துறை விசாரணையின் இலக்காக ஆகிறது.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• கட்டணம்/பணம் செலுத்துவதற்காகப் பணத்தைப் பெற அல்லது மாற்ற உங்கள் கணக்கைப் பயன்படுத்த பிறரை அனுமதிக்காதீர்கள்.

• உங்கள் வங்கிக் கணக்கு விவரங்களைக் கோரிடும் மின்னஞ்சல்களுக்கு பதிலளிக்க வேண்டாம்.

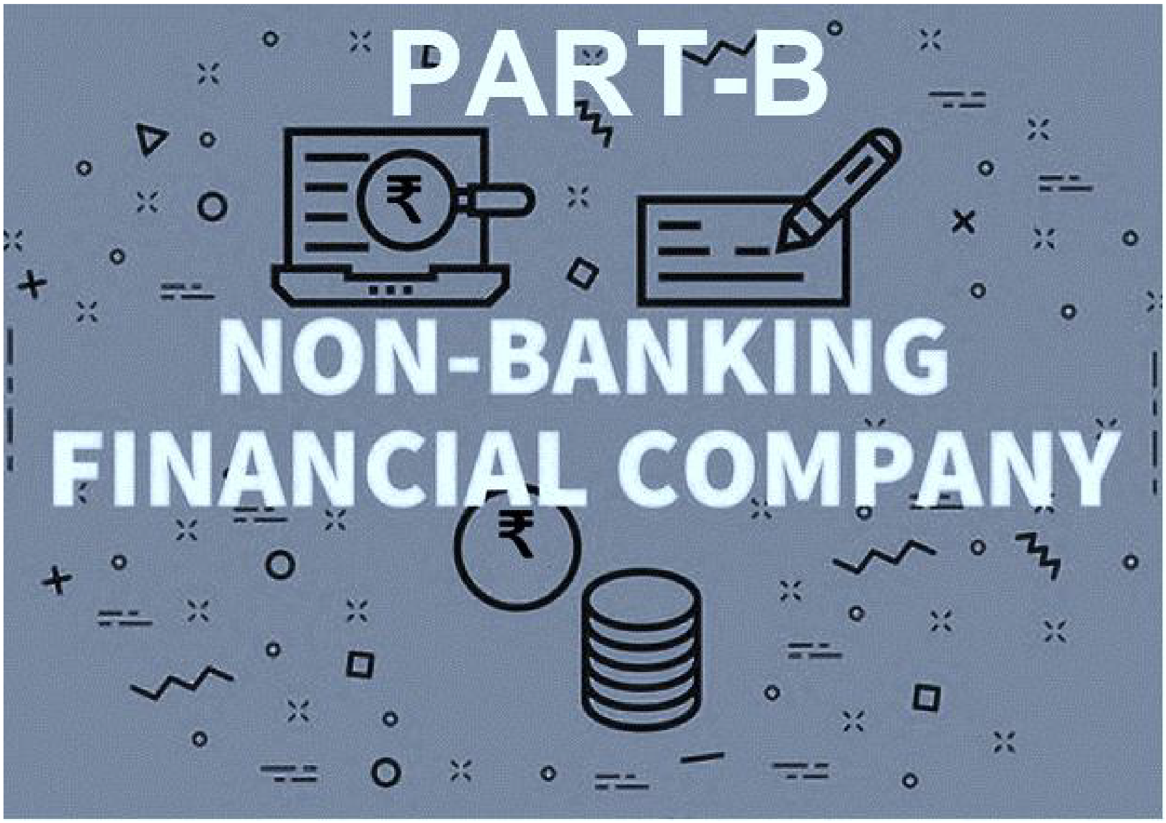
• கவர்ச்சிகரமான சலுகைகள் / கழிவுத்தொகைகள் மூலம் ஏமாற்றப் பட்டு, அங்கீகரிக்கப்படாத பணத்தைப் பெறுவதற்கும், அவற்றை மற்ற வர்களுக்கு மாற்றுவதற்கும் அல்லது பணத்தைப் பெற்றுக்கொண்டு அதற்கான கட்டணத்திற்கு வழங்குவதற்கும் ஒப்புதல் அளிக்காதீர்கள்.

• நிதி ஆதாரம் உண்மையானதாக இல்லாவிட்டால், அல்லது அடிப்படை பரிமாற்றம் செய்வதற்கான காரணம் அதிகாரிகளிடம் நிரூபிக்கப்படா

விட்டால், பணத்தைப் பெறுபவர் காவல்துறையில்புகாரளித்தல் போன்ற பிற சட்டநடவடிக்கை களை இந்நிறுவனங்கள் கடுமையான சிக்கலில் இறங்கக்கூடும்.

விழிப்(புடன்)பாய் இருந்திடுவதற்கான செயல் முறைகளும் மோசடி பரிமாற்றங்களுக்கு எதிராக எடுக்க வேண்டிய முன்னெச்சரிக்கை நடவடிக்கைகளும் - வங்கி அல்லாத நிதி நிறுவனங்கள் (NBFCs)

பகுதி - ஆ(Part -B) - வங்கி அல்லாத நிதி நிறுவனங்கள் (NBFCs)



…

1.மோசடி செய்பவர்களின் கடனை நீட்டிப்பதற்கான போலியான விளம்பரங்கள்



…

செயல் முறை

• மோசடி செய்பவர்கள் தனிநபர் கடன்களை மிகவும் கவர்ச்சிகரமான குறைந்த வட்டி விகிதங்களில் அல்லது எளிதாக திருப்பிச் செலுத்தும் வாய்ப்புஅல்லது பிணையம்/பாதுகாப்பு போன்றவைகளுக்காக தேவையில்லாமல் போலியான விளம்பரங்களை வெளியிடுகின்றனர்.

• மோசடி செய்பவர்கள் அத்தகைய சலுகைகளுடன் மின்னஞ்சல்களை அனுப்புகிறார்கள் கடன் வாங்குபவர்களைத் தொடர்பு கொள்ளுமாறு கேட்டுக்கொள்கிறார்கள். ஏமாறக்கூடிய கடன் வாங்குபவர்களிடம் நம்பகத்தன்மையைப் பெறுவதற்கும் நம்பிக்கையைத் தூண்டுவதற்கும், இந்த மின்னஞ்சல் முகவரிகள் நன்கு அறியப்பட்ட / உண்மையான வங்கி சாரா நிதி நிறுவனங்களின் (NBFCs) மூத்த அதிகாரிகளின் மின்னஞ்சல் முகவரிகளைப் போன்று தோற்றமளிக்கின்றன.

• கடன் பெறுபவர்கள் கடனுக்காக மோசடி செய்பவர்களை அணுகும் போது, மோசடி செய்பவர்கள், செயலாக்க கட்டணம், சரக்கு சேவை வரி (சசேவ(GST)), நகரங்களுக்கு இடையேயான போக்குவரத்துக்கட்டணம், முன்பணம், சமமான மாதாந்திர தவணை (EMI) போன்ற பல்வேறு முன்கூட்டிய கட்டணங்களின் பெயரில் கடன் வாங்கியவர்களிடமிருந்து பணத்தைப் பெறுகிறார்கள்.ஆனால் அவ்வாறானவர்களுக்கான கடன்தொகையினை வழங்காமல் தலைமறைவாகிவிடுவார்கள்.

• மோசடி செய்பவர்கள், பொதுமக்கள் கடன்கள் பற்றிய தகவல்களைத் தேடும்போது, தேடுபொறிகளில் காண்பிக்க போலியான இணையதள இணைப்புகளையும் உருவாக்குகிறார்கள்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• NBFCகள் / வங்கிகளால் விதிக்கப்படும் கடன் செயலாக்கக் கட்டணம், அனுமதிக்கப்பட்ட கடன் தொகையிலிருந்து கழிக்கப்படும், மேலும் கடன் வாங்குபவரிடம் இருந்து ரொக்கமாக முன்பணமாகக் கோரப்படுவதில்லை.

• எந்தவொரு செயலாக்கக் கட்டணத்தையும் முன்கூட்டியே செலுத்த வேண்டாம், ஏனெனில் NBFCகள் / வங்கிகள் கடன் விண்ணப்பத்தைச் செயலாக்குவதற்கு முன் ஒருபோதும் முன்கூட்டிய கட்டணத்தைக் கோராது.அவ்வாறான கட்டணங்களை கடன்வழங்கிடும் தொகையில் கழித்துகொள்வார்கள் என்ற செய்தியை மனதில்கொள்க

• உண்மையான ஆதாரங்கள் மூலம் விவரங்களைச் சரிபார்க்காமல்/ ஒப்பிடாமல், குறைந்த வட்டி விகிதத்தில் கடன்களை இணையத்தில் வழங்குவதற்கு எதிராக பணம் செலுத்தவோ அல்லது பாதுகாப்பு சான்றிதழ்களை உள்ளிடவோ வேண்டாம்.

2.குறுஞ்செய்தி / மின்னஞ்சல் / உடனடி செய்தி அனுப்புதல் / அழைப்பு மோசடிகள்



…

செயல் முறை

• மோசடி செய்பவர்கள் கவர்ச்சிகரமான கடன்களில் உடனடி செய்திக்கான பயன்பாடுகள் / குறுஞ்செய்தி / சமூக ஊடக தளங்களில் போலி செய்திகளைப் பரப்புகிறார்கள், நம்பகத்தன்மையைத் தூண்டுவதற்காக அவர்கள் பகிரும் கைபேசி எண்ணில் அறியப்பட்ட எந்த NBFC யின் வர்த்தக முத்திரையையும் சுயவிவரப் படமாகப் பயன்படுத்திகி கொள்கிறார்கள்.

• மோசடி செய்பவர்கள் தங்களுடைய ஆதார் அட்டை / வருமானவரி அட்டை,,போலியானNBFCஇன் அடையாள அட்டையை கூட பகிர்ந்து கொள்ளலாம்.

• இத்தகைய மொத்தசெய்திகளை/ குறுஞ்செய்திகளை/ மின்னஞ்சல் களை அனுப்பிய பிறகு,மோசடி செய்பவர்கள் **ஏதேனும்/குறிப்பற்ற (Random)**நபர்களை அழைத்து,போலியான அனுமதி கடிதங்கள்,போலியான காசோலைகளின் நகல்கள் போன்றவற்றைப் பகிர்ந்துகொண்டு பல்வேறு கட்டணங்களைக் கோருகின்றனர். கடன் வாங்கியவர்கள் இந்தக் கட்டணத்தைச் செலுத்தியவுடன், மோசடி செய்பவர்கள் பணத்துடன் தலைமறைவாகின்றார்கள்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• தொலைபேசிகள் / மின்னஞ்சல்கள் போன்றவற்றின் மூலம் மக்கள் நேரடியாக வழங்கும் கடன் சலுகைகளை ஒருபோதும் நம்ப வேண்டாம்.

• இதுபோன்ற சலுகைகளுக்கு எதிராக எந்தப் பணமும் செலுத்த வேண்டாம் அல்லது பிற ஆதாரங்கள் மூலம் உண்மையானதா என்று குறுக்கு சோதனை செய்யாமல், அத்தகைய சலுகைகளுக்கு எதிராக எந்தவொரு தனிப்பட்ட/நிதிபாதுகாப்புச் சான்றுகளையும் பகிர வேண்டாம்.

• குறுஞ்செய்திகள்(SMS)/ மின்னஞ்சல்கள் மூலம் அனுப்பப்படும் இணைப்புகளை சொடுக்குதல் செய்யாதீர்கள் அல்லது விளம்பர SMS / மின்னஞ்சல்களுக்கு பதிலளிக்க வேண்டாம்.

• சந்தேகத்திற்கிடமான இணைப்பு அல்லது மோசடி**(phishing)** இணைப்புகளைக் கொண்ட அறியப்படாத மூலங்களிலிருந்து வரும் மின்னஞ்சல்களைத் திறக்கவோ / பதிலளிக்கவோ வேண்டாம்.

3.ஒருமுறைமட்டுமானகடவுச்சொல்(OTP) அடிப்படையிலான மோசடிகள்



…

செயல் முறை

• NBFC போன்று ஆள்மாறாட்டம் செய்யும் மோசடி செய்பவர்கள்,

கடன்கள் அல்லது NBFC/வங்கி வாடிக்கையாளர்களின் கடன் கணக்குகளில்

கடன் வரம்பை அதிகரிக்கச் செய்து SMS/செய்திகளை அனுப்பி, வாடிக்கையாளர்களை கைபேசி எண்ணில் தொடர்பு கொள்ளச் செய்வார்கள்.

• வாடிக்கையாளர்கள் அத்தகைய எண்களை அழைக்கும் போது, மோசடி செய்பவர்கள் தங்களுடைய நிதிச் சான்றுகளை சேகரிக்க படிவங்களை நிரப்பச் சொல்கிறார்கள். மோசடி செய்பவர்கள் OTP அல்லது PIN விவரங்களைப் பகிர்ந்து கொள்ளும்படி வாடிக்கையாளர்களைத் தூண்டுகிறார்கள் / நம்பவைக்கிறார்கள், தொடர்ந்து வாடிக்கையாளர்களின் கணக்குகளில் இருந்து அங்கீகரிக்கப்படாத பரிமாற்றங்களைச் செய்கிறார்கள்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

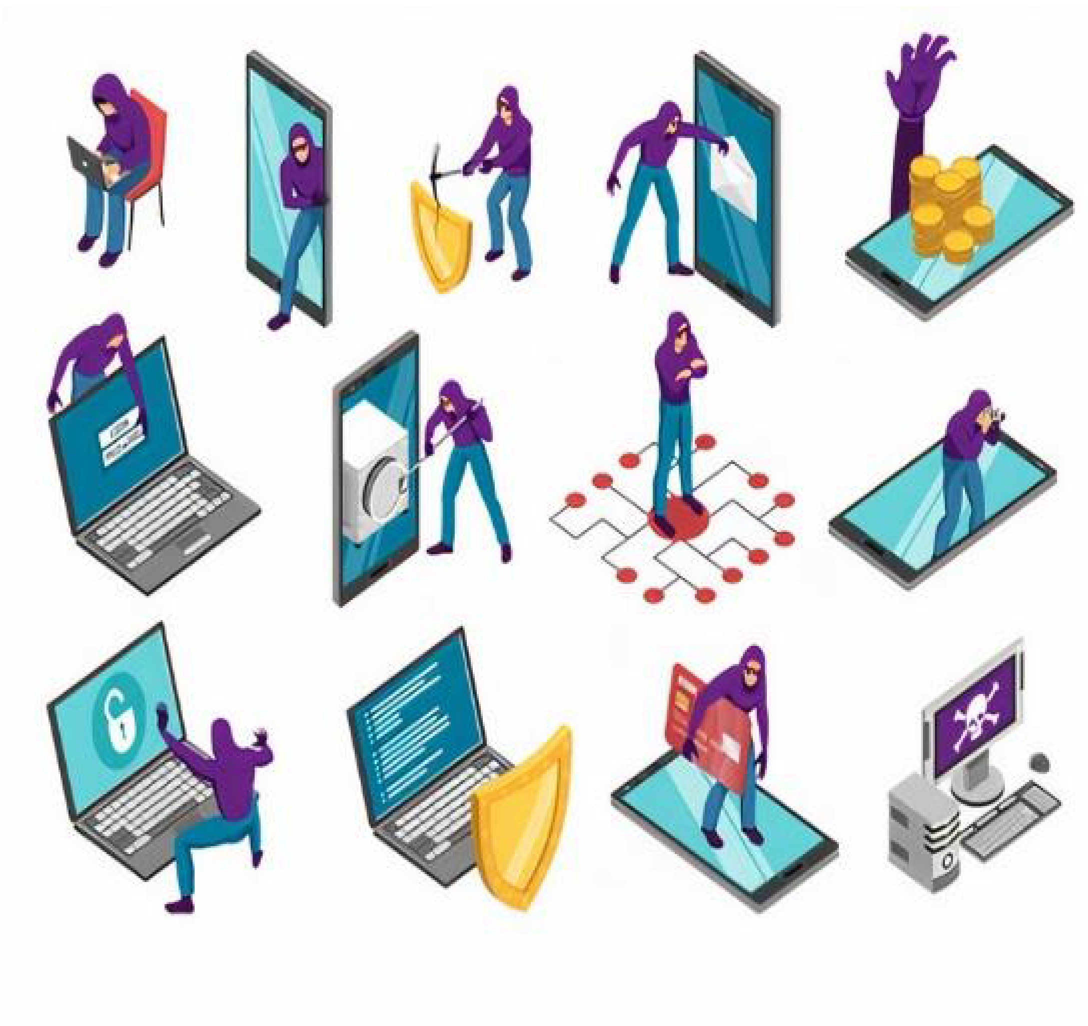
• OTP / PIN / தனிப்பட்ட விவரங்கள், முதலியவற்றை, உங்கள் சொந்த நண்பர்கள் குடும்ப உறுப்பினர்கள் உட்பட யாருடனும் எந்த வடிவத்திலும் பகிர்ந்துகொள்ள வேண்டாம்.

• உங்களிடம்முன்கூட்டியேதெரிந்துகொள்ளாமல் OTP உருவாக்கப் படவில்லை என்பதை உறுதிப்படுத்த SMS / மின்னஞ்சல்களை தவறாமல் சரிபார்த்திடுக.

• வங்கி / NBFC / e-wallet வழங்குநரின் அதிகாரப்பூர்வ வலைத்தளத்தை எப்போதும் அணுகவும் அல்லது அவர்களின் சேவைகளைப் பெற

தொடர்புடைய கிளையைத் தொடர்பு கொள்க / அல்லது உற்பத்தி, சேவைகள் தொடர்பான தகவல், தெளிவுபடுத்தல்களைப் பெற்றிடுக

4.போலியான கடன் வழங்கிடும்இணையதளங்கள் / பயன்பாட்டு மோசடிகள்



…

செயல் முறை

• மோசடி செய்பவர்கள் நேர்மையற்ற கடன் பயன்பாடுகளை உருவாக்குகிறார்கள், அவை உடனடியாகம் குறுகிய கால கடன்களை வழங்குகின்றன. இந்த பயன்பாடுகள் கடன் வாங்குபவர்களை ஏமாற்றுவதோடு, அதிக வட்டி விகிதங்களையும் வசூலிக்கக்கூடும்.

• ஏமாறக்கூடிய கடன் வாங்குபவர்களை ஈர்க்க, மோசடி செய்பவர்கள் "வரையறுக்கப்பட்ட குறுகியகால சலுகைகளை" விளம்பரப்படுத்து கிறார்கள் கடன் வாங்குபவர்களை நெருக்கடியானநிலையில் தந்திரங்களைப் பயன்படுத்தி அவசரமாக முடிவுகளை எடுக்குமாறு நெருக்குதல் கொடுக்கின்றனர்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• கடன் வழங்குபவர் அரசிடம் / கட்டுபாட்டாளரிடம் / அங்கீகரிக்கப்பட்ட முகவர்களிடம் பதிவு செய்திருக்கிறாரா என்பதை சரிபார்த்திடுக

• கடன் வழங்குபவர் **உண்மையான**முகவரி அல்லது தொடர்புத் தகவலை வழங்கியுள்ளாரா என்பதைச் சரிபார்த்திடுக, பின்னர் அவர்களைத் தொடர்புகொள்வது கடினம் அன்று என்பதை உறுதிப்படுத்திடுக.

• கடன் வழங்குபவர் கடன்தகுதிசான்றினைச் சரிபார்ப்பதை விட தனிப்பட்ட விவரங்களைப் பெறுவதில் அதிக ஆர்வம் காட்டினால் எச்சரிக்கையாக இருந்திடுக.

• எந்தவொரு புகழ்பெற்ற NBFCயும் / வங்கியும் கடன் விண்ணப்பத்தை செயலாக்குவதற்கு முன் ஒருபோதும் கட்டணம் செலுத்திடுமாறுகோராது என்பதை நினைவில் கொள்க.

• உண்மையான கடன் வழங்குநர்கள் கடனாளிகளின் ஆவணங்களை பிற சான்றுகளை சரிபார்க்காமல் பணத்தை வழங்க மாட்டார்கள்.

• இந்த NBFC-ஆதரவு பெற்ற கடன் பயன்பாடுகள் உண்மையானவைகளா என்பதையும் சரிபார்த்திடுக.

5.பணப் புழக்கம் / Ponzi/ பல்லடுக்குநிலைசந்தைபடுத்துதல் (MLM) திட்டங்களின் மோசடி



...

செயல் முறை

• மோசடி செய்பவர்கள் பல்லடுக்கநிலைசந்தைபடுத்துதல்(Multi-Level Marketing (MLM)) / சங்கிலித்தொடர் போன்று சந்தைபடுத்துதல் / கோபுரம் போன்ற கட்டமைப்பு திட்டங்களைப் பயன்படுத்தி, உறுப்பினர்களை இணைக்கும்போது /சேர்க்கும்போது எளிதாக அல்லது விரைவாக பணம்பெறுவதை உறுதியளிக்கின்றனர்.

• இந்தத் திட்டங்கள் அதிக வருமானத்தை உறுதி செய்வதோடு மட்டுமல்லாமல், ஏமாறும் நபர்களின் நம்பிக்கையைப் பெறவும், வாய்வழியிலான விளம்பரம் மூலம் அதிக முதலீட்டாளர்களை ஈர்க்கவும் முதலில் சில தவணைகளை (EMIகள்) செலுத்துகின்றன.

• இந்தத் திட்டங்களின் சங்கிலியில் / குழுவில் அதிக நபர்களைச் சேர்ப்பதை ஊக்குவிக்கின்றன. பொருட்களை விற்பனை செய்வதை விட, திட்டத்தில் சேரும் நபர்களின் எண்ணிக்கைக்கு, பதிவு செய்தவருக்கு கழிவுத்தொகை கூடுதலாக வழங்கப்படுகிறது.

• திட்டத்தில் சேரும் நபர்களின் எண்ணிக்கை குறையத் தொடங்கும் போது இந்த மாதிரியான மோசடியானது சில காலத்திற்குப் பிறகு நீடிக்க முடியாததாகிவிடுகின்றது. அதன்பிறகு, மோசடி செய்பவர்கள் அந்த திட்டத்தையே மூடிவிட்டு, அதுவரை மக்கள் முதலீடு செய்த பணம் அனைத்தையும் எடுத்து கொண்டு காணாமல் போய்விடுகின்றனர்

முன்னெச்சரிக்கை நடவடிக்கைகள்

• வருமானமும் இழப்புஆபத்துகளும் நேரடிவிகிதாசார தொடர்புடையதாகும். அதிக வருமானம், அதிக ஆபத்துகொண்டதாகும்.

• வழக்கத்திற்கு மாறாக அதிக வருமானத்தை (ஆண்டொன்றிற்கு40-50%) தொடர்ந்து வழங்கும் எந்தவொரு திட்டமும், சாத்தியமான மோசடிக்கான முதல் அறிகுறியாக இருக்கலாம், எச்சரிக்கையாக இருக்க வேண்டும்.

• பொருட்களின்/சேவையின் உண்மையான விற்பனை இல்லாமல் ஏதேனும் கட்டணம் / கழிவுத்தொகை / ஊக்கத்தொகை / இலாபத்தின் பங்கு சதவீதம் என்பது சந்தேகத்திற்குரியது , மோசடிக்கு வழிவகுக்கும் என்பதால் இவ்வாறானசெயல்களை மிகச்சரியாக கவனித்திடுக.

• பல்லடுக்கநிலைசந்தைபடுத்துதல்(Multi-Level Marketing (MLM)) / சங்கிலி தொடர் போன்று சந்தைபடுத்துதல் / கோபுரம்போன்ற கட்டமைப்பு திட்டங்களை இயக்கும் நிறுவனங்களால் வழங்கப்படும் அதிக வருமானம் பற்றிய வாக்குறுதிக்க எப்போதும்ஆசைப்பட வேண்டாம்.

• பணச் சுழற்சி / பல்லடுக்குநிலை சந்தைப்படுத்தல் / கோபுர கட்டமைப்பு களின் கீழ் பணத்தை ஏற்றுக்கொள்வது பரிசு சீட்டுகள் ,

பணச் சுழற்சித் திட்டங்கள் (தடை) சட்டம்,1978 இன்கீழ் குற்றசெயலாகும்.

• அத்தகைய சலுகைகள் அல்லது அத்தகைய திட்டங்களின் தகவல்கள் இருந்தால், உடனடியாக மாநில காவல்துறையில் புகார் அளித்திடுக.

6.போலி ஆவணங்களின் மூலமான மோசடியான கடன்



…

செயல் முறை

• மோசடி செய்பவர்கள் நிதி நிறுவனங்களிடமிருந்து சேவைகளைப் பெற போலி ஆவணங்களைப் பயன்படுத்துகின்றனர்.

• மோசடி செய்பவர்கள் அடையாளத் திருட்டுகள், அடையாள அட்டைகள், வங்கிக் கணக்கு விவரங்கள் போன்ற வாடிக்கையாளர்களின் தனிப்பட்ட தகவல்களைத் திருடுகிறார்கள், மேலும் நிதி நிறுவனத்திலிருந்து பலன்களைப் பெற இந்தத் தகவல் அல்லது பாதுகாப்பு சான்றிதழை பயன்படுத்துகின்றனர்.

• மோசடி செய்பவர்கள் NBFC ஊழியர்களாகக் காட்டிகொண்டு, வாடிக்கை யாளர் களிடமிருந்து KYC தொடர்பான ஆவணங்களைச் சேகரிக்கின்றனர்.

முன்னெச்சரிக்கை நடவடிக்கைகள்

• எந்தவொரு நிறுவனத்திடமிருந்தும், குறிப்பாக இந்த நிறுவனங்களின் பிரதிநிதிகளாகக் காட்டிக் கொள்ளும் தனிநபர்களிடமிருந்து கடன் அனுமதி / கடன் வசதியைப் பெறுவதற்கான தேசிய தானியங்கி தீர்வுஇல்ல (National Automated Clearing House (NACH)) படிவம் உட்பட KYC விவரங்களை, பிற தனிப்பட்ட ஆவணங்களை வழங்கும்போது உரிய கவனித்தலையும் விழிப்புணர்வையும் கடைப்பிடித்திடுக.

• அத்தகைய ஆவணங்கள் நிறுவனத்தின் அங்கீகரிக்கப்பட்ட பணியாளர்கள் அல்லது நிறுவனங்களின் அங்கீகரிக்கப்பட்ட மின்னஞ்சல் முகவரிகளில் மட்டுமே பகிர்ந்துகொள்ளப்பட வேண்டும்.

• கடனை அனுமதிக்காத பட்சத்தில் / அல்லது கடன் கணக்கை முடிவுக்கொண்டுவந்தபின்னர், நீங்கள் பகிர்ந்துள்ள ஆவணங்கள்

உடனடியாக நீக்கிவிடுவதை உறுதிசெய்ய, சம்பந்தப்பட்ட நிறுவனங்களைப் பின்தொடர்ந்து அறிந்துகொள்க.

நிதி பரிமாற்றங்களின்போது எடுக்க வேண்டிய பொதுவான முன்னெச்சரிக்கை நடவடிக்கைகள்

பகுதி - இ



…

1.பொதுவான முன்னெச்சரிக்கை நடவடிக்கைகள்



...

• இணையத்தில் உலாவிடும் போது தோன்றும் சந்தேகத்திற்கிடமான மேல்மீட்புபட்டிகள்(pop ups) குறித்து எச்சரிக்கையாக இருந்திடுக.

• இணையத்தில் பணம் செலுத்துவதற்கு / பரிமாற்றம் செய்வதற்கு முன் எப்போதும் பாதுகாப்பான கட்டண நுழைவாயிலை (https:// - பூட்டு முத்திரையுடன் கூடிய இணையதள(UR)Lமுகவரியை சரிபார்த்திடுக.

• PIN (தனிப்பட்ட அடையாள எண்), கடவுச்சொல் , கடனட்டை அல்லது பற்றட்டை எண், CVV போன்றவற்றை தனிப்பட்ட பாதுகாப்புமுறையில் வைத்திடுக வங்கிகள்/நிதி நிறுவனங்கள், நண்பர்கள் அல்லது குடும்ப உறுப்பினர்களுடன்கூட இரகசிய நிதித்தகவலைப் பகிர்ந்துகொள்ள வேண்டாம்.

• இணையதளங்களில்/சாதனங்களில் / பொது மடிக்கணினிகளில் / மேசைக்கணினிகளில் அட்டை விவரங்களைச் சேமிப்பதைத் தவிர்த்திடுக.

• அத்தகைய வசதி கிடைக்கும் இடத்தில் இரு காரணி அங்கீகாரத்தை செயல்படுதிதிடுக

. • சந்தேகத்திற்கிடமான இணைப்பு அல்லது மோசடி(Phising) இணைப்புகளாக இருக்கலாம் என்பதால், அறியப்படாத மூலங்களிலிருந்து வரும் மின்னஞ்சல்களைத் திறக்கவோ / பதிலளிக்கவோ வேண்டாம்.

• காசோலை புத்தகம், KYC ஆவணங்களின் நகல்களை அந்நியர்களுடன் பகிர்ந்து கொள்ள வேண்டாம்.

2.சாதனத்தின் / கணினியின் பாதுகாப்பிற்காக



...

• கடவுச்சொற்களை சீரான இடைவெளியில் மாற்றியமைத்திடுக

. • உங்கள் சாதனங்களில் எதிர்நச்சுநிரலை**(antivirus)** நிறுவுகைசெய்து, கிடைக்கும் போதெல்லாம் புதுப்பிப்புகளை நிறுவுகைசெய்திடுக.

• எப்போதும் அறியப்படாத விரலியின்(Universal Serial Bus (USB)) இயக்கிகள் / சாதனங்களைப் பயன்படுத்துவதற்கு முன்பு வருடுதல் செய்திடுக.

• உங்கள் சாதனத்தைத் திறந்தநிலையில் விட்டிட்டு வேறிடம்செல்லாதீர்கள்.

• ஒரு குறிப்பிட்ட நேரத்திற்குப் பிறகு சாதனத்தின் தானாக பூட்டிடுமாறு உள்ளமைத்திடுக.

• உங்கள் கைபேசியில் / மடிக்கணினியில் அறியப்படாத பயன்பாடுகள் அல்லது மென்பொருளை நிறுவுகைசெய்திட வேண்டாம்.

• கடவுச்சொற்கள் அல்லது இரகசிய தகவல்களை சாதனங்களில் சேமிக்க வேண்டாம்.

3.பாதுகாப்பான இணைய உலாவலுக்கு

• பாதுகாப்பற்ற / ஆபத்தற்ற / அறியப்படாத இணையதளங்களைப் பார்வையிடுவதைத் தவிர்த்திடுக.

• தெரியாத இணையஉலாவிகளைப் பயன்படுத்துவதைத் தவிர்த்திடுக.

• பொது சாதனங்களில் கடவுச்சொற்களைப் பயன்படுத்துவதை / சேமிப்பதைத் தவிர்த்திடுக.

• தெரியாத இணையதளங்களில்/பொது சாதனங்களில் பாதுகாப்பு சான்றுகளை உள்ளிடுவதை தவிர்த்திடுக.

• தனிப்பட்ட தகவல்களை யாருடனும், குறிப்பாக சமூக ஊடகங்களில் தெரியாத நபர்களுடன் பகிர்ந்துகொள்ள வேண்டாம்.

• எந்தவொரு இணையப்பக்கத்தின் பாதுகாப்பையும் எப்போதும் சரிபார்த்திடுக (https:// - பூட்டுமுத்திரையுடன் கூடிய URL), மேலும் ஒரு மின்னஞ்சல் அல்லது SMS இணைப்பு அத்தகைய பக்கங்களுக்கு

திருப்பி விடப்படும் போது கண்டிப்பாக பாதுகாப்பினை சரிபார்த்திடுக.

4.பாதுகாப்பான இணைய வங்கிஉலாவலுக்கு



…

• பொது சாதனங்களில் எப்போதும் மெய்நிகர் விசைப்பலகையைப் பயன்படுத்திடுக, ஏனெனில் விசைகளின் அழுத்தங்களை ஒத்திசைவு செய்யப்பட்ட சாதனங்கள், விசைப்பலகை போன்றவற்றின் மூலமாகவும் கைப்பற்ற முடியும்.

• பயன்பாட்டிற்குப் பிறகு உடனடியாக இணைய வங்கி அமர்விலிருந்து வெளியேறிடுக.

• கடவுச்சொற்களை அவ்வப்போது புதுப்பித்திடுக.

• உங்கள் மின்னஞ்சல் , இணைய வங்கி ஆகிய இரண்டிற்கும் ஒரே கடவுச்சொற்களைப் பயன்படுத்த வேண்டாம்.

• நிதி பரிமாற்றங்களுக்கு பொது முனைமங்களை (அதாவது மின்வெளிஉணவகம்(**cyber cafe)** போன்றவை) பயன்படுத்துவதை தவிர்த்திடுக

5.கைபேசி உளவு பார்க்கப்படுவதைக் குறிக்கும் காரணிகள்

• அறிமுகமில்லாத பயன்பாடுகள் கைபேசியில் பதிவிறக்கம் செய்யப்படுகின்றன.

• கைபேசி மின்கலன் வழக்கத்தை விட வேகமாக வடிகட்டப்படுகிறது.

• கைபேசி சூடாகஆவது பின்னணியில் உளவாளியை இயக்குவதன் மூலம் யாரோ உளவு பார்ப்பதற்கான அறிகுறியாக இருக்கலாம்.

• தரவு நுகர்வு அளவு ஒரு அசாதாரணஉயர்வானது சில நேரங்களில் ஒரு உளவாளி பின்னணியில் இயங்குகின்ற ஒரு அறிகுறியாக இருக்கலாம்.

• உளவாளி பயன்பாடுகள் சில சமயங்களில் கைபேசிசெயலை நிறுத்திடும் செயலில் குறுக்கிடலாம், இதனால் சாதனம் சரியாக அனைக்கப்படாது அல்லது வழக்கத்திற்கு மாறாக நீண்ட நேரம்

எடுக்கும். • உரைச் செய்திகளை உளவாளி **malware** மூலம் தரவுகளை அனுப்பவும் பெறவும் பயன்படுத்தலாம் என்பதை நினைவில் கொள்க.

6.மோசடி நடந்த பிறகு எடுக்க வேண்டிய நடவடிக்கைகள்

• பற்றுஅட்டையின் /கடனட்டையின் செயலைத் தடுப்பது மட்டு மல்லாமல், உங்கள் வங்கியின் கிளைக்குச் சென்று அல்லது வங்கியின் இணைய தளத்தில் கிடைக்கும் அதிகாரப்பூர்வ வாடிக்கையாளர் சேவை எண்ணை அழைப்பதன் மூலம் அட்டையுடன் இணைக்கப்பட்ட வங்கிக் கணக்கில் உள்ள பற்றினை முடக்கிடுக. மேலும், ஒரு மோசடியைத் தொடர்ந்து பற்று/கடன் அட்டைகள் தடுக்கப்பட்டவுடன், மோசடி நிரந்தரமாகத் தடுக்க, இணையவங்கி, கைபேசிசெயலி போன்ற பிற வங்கிஇணைப்பு**களின்(channels)** பாதுகாப்பை சரிபார்த்து உறுதிப்படுத்திடுக.

• உதவிஎண் 155260 அல்லது 1930 ஐ தொடர்புகொள்க அல்லது தேசிய மின்வெளிகுற்ற(Cybercrime)அறிக்கையிடல் தளத்தில் (www.cybercrime.gov.in) சம்பவத்தைப் புகாரளித்திடுக.

கைபேசியை மீட்டமை: கைபேசியில் இருந்து தரவு கசிவு காரணமாக மோசடி நடந்தால் கைபேசியை மீட்டமைக்க Setting-Reset-Factory Data

என்பதை பயன்படுத்திடுக.

7.பற்று /கடன் அட்டைகள் தொடர்பான முன்னெச்சரிக்கைகள்

• **.பற்று /கடன் அட்டையி**ன்**(Debit / Credit card)** பல்வேறு வசதிகளை நீங்கள் செயலிழக்கச் செய்ய வேண்டும்.

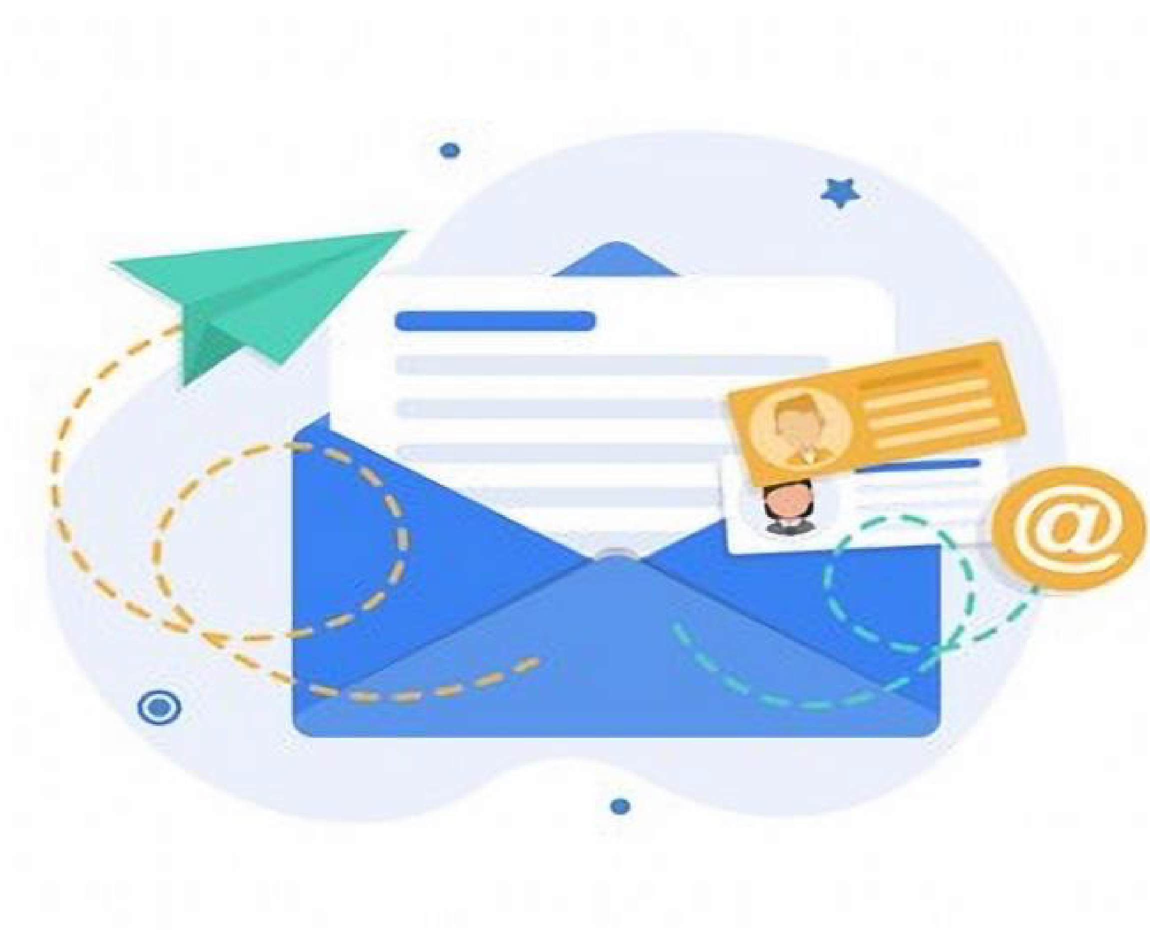
• இதேபோன்று, அட்டையைப் பயன்படுத்தக் கூடாது என்றால், அருகாமை புலத்தொடர்பு (Near Field Communication (NFC))வசதி செயலிழக்கப்பட வேண்டும்.

• ஏதேனும் ஒரு விற்பனைமுனையத்தில் (POS) PIN ஐ உள்ளிடுவதற்கு முன் அல்லது NFC படிப்பானில் அட்டையைப் பயன்படுத்தும் போது, POS இயந்திரத் திரை , NFCபடிப்பானில் காட்டப்படும் தொகையை நீங்கள் கவனமாகச் சரிபார்த்திடுக.

• பரிமாற்றம் செய்யும் போது அட்டையை தேய்த்திடுவதற்காக உங்கள் பார்வையில் இருந்து அட்டையை எடுத்துச் செல்ல வணிகநபரை ஒருபோதும் அனுமதிக்காதீர்கள்.

• POS தளம் / ATMஇல் PIN ஐ உள்ளிடும்போது உங்கள் மற்றொரு கையால் விசைப்பலகைய மூடிமறைத்திடுக.

8.மின்னஞ்சல் கணக்கின் பாதுகாப்பிற்காக



...

• தெரியாத முகவரிகள் / பெயர்கள் மூலம் மின்னஞ்சல்கள் மூலம் அனுப்பப்படும் இணைப்புகளை எப்போதும் சொடுக்குதல் செய்ய வேண்டாம்.

• பொது அல்லது இலவச இணையஇணைப்புகளில் மின்னஞ்சல்களைத் திறப்பதைத் தவிர்த்திடுக

. • பாதுகாப்பான சான்றுகள் / வங்கி கடவுச்சொற்கள் போன்றவற்றை மின்னஞ்சல்களில் சேமிக்க வேண்டாம்.

9.கடவுச்சொற்களின் பாதுகாப்பிற்காக



…

• உங்கள் கடவுச்சொல்லில்(password) எண்கள் எழுத்துகள் , சிறப்புகுறியீடுகள் ஆகியவற்றினை கலந்து பயன்படுத்திடுக.

• உங்கள் எல்லா கணக்குகளுக்கும் இரண்டு காரணி அங்கீகார(two factor authentication)வசதி இருந்தால் அத்தகையை வசதியை அமைத்திடுக,.

• உங்கள் கடவுச்சொற்களை அவ்வப்போது மாற்றிகொண்டேயிருந்திடுக.

• உங்கள் பிறந்த தேதி, மனைவியின் பெயர், கார் எண் போன்றவற்றை கடவுச்சொற்களாக வைத்திருப்பதைத் தவிர்த்திடுக

10.NBFC ஆல்ஏற்றுக்கொள்ளும் வைப்புத்தொகை உண்மையானதா இல்லையா என்பதை எப்படி அறிவது?



…

• https://rbi.org.in இல் கிடைக்கும் வைப்புத்தொகைகளை ஏற்கும் வைப்புத்தொகைவாங்கிடும் உரிமையுள்N NBFCகளின் பட்டியலில் NBFC இன் பெயர் உள்ளதா என்பதைச் சரிபார்த்து,வைப்புத்தொகைகளை ஏற்கத்

தடைசெய்யப்பட்ட நிறுவனங்களின் பட்டியலில் அது இடம்பெறவில்லை என்பதை உறுதிப்படுத்திடுக.

• NBFCக்கள் இந்திய சேமநல (RBI)வங்கியால் வழங்கப்பட்ட பதிவுச் சான்றிதழை (CoR) அதன் தளத்தில் / அதன் அலுவலகத்தில் முக்கியமாகக் காட்ட வேண்டும். வைப்புத்தொகைகளை ஏற்க RBI ஆல் NBFCக்கு குறிப்பாக அங்கீகாரம் வழங்கப்பட்டுள்ளது என்பதையும் இந்தச் சான்றிதழ் பிரதிபலிக்க வேண்டும். வைப்புத்தொகைகளை ஏற்க NBFC அங்கீகரிக்கப்பட்டுள்ளதா என்பதை உறுதிப்படுத்த இந்த சான்றிதழை ஆய்வுசெய்திடுக.

• NBFCகள் 12-மாதங்களுக்கும் குறைவான , 60 மாதங்களுக்கும் மேலான காலத்திற்கு வைப்புத்தொகையை ஏற்க முடியாது ஒரு NBFC ஒரு வைப்புத் தொகையாளருக்கு செலுத்தக்கூடிய அதிகபட்ச வட்டி விகிதம் 12.5% ஐ விட அதிகமாக இருக்கக்கூடாது.

• இந்திய சேமநல வங்கியானது(RBI) வட்டி விகிதங்களின் மாற்றத்தை https://rbi.org.inஎனும் இணையதளமுகவரியில் → Sitemap → NBFC List → FAQs. எனும் அடிக்கடி கேட்கப்படும் கேள்விகளில் வெளியிடுகிறது.

11.வைப்பீடு செய்பவர்கள் எடுக்க வேண்டிய முன்னெச்சரிக்கை நடவடிக்கைகள்



…

• பணத்தை வைப்பீடு செய்யும் போது, வங்கி / NBFC / நிறுவனத்தில் செய்யப்படும் ஒவ்வொரு வைப்பீட்டிற்கும் முறையான ஒப்புகைசீட்டினை வழங்கிடுமாறு வலியுறுத்திடுக.

• ஒப்புகை தாளில் நிறுவனத்தால் அங்கீகரிக்கப்பட்ட அதிகாரி ஒருவரால் முறையாக கையொப்பமிடப்பட வேண்டும், மற்றவற்றுடன், வைப்புத்தொகையின் தேதி, வைப்பீடு செய்தவரின் பெயர்,இதர விவரங்களுடன் தொகை, செலுத்த வேண்டிய வட்டி விகிதம், முதிர்வு தேதி, தொகைஎண்ணாலும் எழுத்தாலும் ஆகியவிவரங்களை கண்டிப்பாகக் குறிப்பிட்டிருக்க வேண்டும்.

• தரகர்கள் / முகவர்கள் போன்றவற்றில், NBFC களின் சார்பாக பொது வைப்புத்தொகைகளை சேகரிக்கும் போது, தரகர்கள் / முகவர்கள் சம்பந்தப்பட்ட NBFC மூலம் முறையாக அங்கீகரிக்கப்பட்டுள்ளனரா என்பதை சரிபார்த்திடுக.

• வைப்புத்தொகை காப்பீட்டு வசதி NBFC களின் வைப்பாளர்களுக்கு இல்லை என்பதை நினைவில் கொள்க

புகார்களை பதிவு செய்தல்

இந்திய நிதிகாப்பகவங்கியின்(RBI)இன்

குறைதீர்ப்பாளரிடம்(Ombudsmen) புகார்அளித்தல்

• இணையத்தில் புகார்களை பதிவு செய்ய, https://cms.rbi.org.in/ என்ற இணைப்பைப் பார்வையிடுக.

• மின்னஞ்சல் மூலம் புகார்களை crpc@rbi.org.in என்ற மின்னஞ்சல் முகவரிக்கு அனுப்பலாம்.

• நேரடியாக/தாள் வடிவில் உள்ள புகார்களை CRPC, இந்திய சேமநல வங்கி(RBI), சென்ட்ரல் விஸ்டா, செக்டர் -17, சண்டிகர் -160 017 என்ற முகவரிக்கு அனுப்பலாம். இந்திய பங்குகளின் , பரிமாற்ற வாரியத்திற்கு (SEBI) புகார் அனுப்பலாம்

• https://www.sebi.gov.in/ என்ற இணைப்பைப் பார்வையிடுக. இந்திய காப்பீட்டு ஒழுங்குமுறை, மேம்பாட்டு ஆணையத்திடம் (IRDAI) புகார் செய்திடுக

• https://www.irdai.gov.in/ என்ற இணைப்பைப் பார்வையிடுக. தேசிய வீட்டுவசதி வங்கிக்கு (NHB) புகார் செய்திடுக

• https://nhb.org.in/ இல் உள்ள இணைப்பைப் பார்வையிடுக மின்வெளி காவல்(CyberCrimePolice) நிலையத்தில் புகார் செய்திடுக

• https://cybercrime.gov.in/ ஐப் பார்வையிடுக

பகுதி- ஈ -.சொற்களஞ்சியம்

• **முன்கூட்டிய கட்டணம்/செயலாக்கக் கட்டணம்/நுழைவு கட்டணம்(Advance fee/Processing fee/Token fee):** ஆவணக் கட்டணங்கள், சந்திப்புச் செலவுகள், செயலாக்கக் கட்டணம், கடன் வாங்குபவருக்குக் கடனை வழங்குவதற்குப் பொருந்தக்கூடிய பிற கட்டணங்கள் போன்ற பூர்வாங்கக் கட்டணங்கள் இதில் அடங்கும்.

• **இரு-காரணி அங்கீகாரம்(Two-factor authentication):** அங்கீகார முறைகளில் மூன்று அடிப்படை 'காரணிகள்' அடங்கும்- பயனருக்குத் தெரிந்த ஒன்று (எ.கா., கடவுச்சொல், PIN- நிலையான அல்லது ஒரு முறை உருவாக்கப் பட்டது); பயனரிடம் உள்ள ஒன்று (எ.கா.,ATM/ திறன்மிகுஅட்டை எண், காலாவதி தேதி அட்டையில் அச்சிடப்பட்ட CVV); , பயனரின் ஏதோ ஒன்று (எ.கா., கைரேகை போன்ற உயிரளவை(biometric) பண்பு). இரண்டு-காரணி அங்கீகாரம் (2FA என்றும் அழைக்கப்படுகிறது) இரண்டு வெவ்வேறு கூறுகளின் கலவையின் மூலம் பயனர்களை அடையாளப் படுத்துகிறது - பயனாளரிடம் என்ன இருக்கிறது , பயனாளர் அறிந்தவை/ பரிமாற்றத்தினை முடிக்க வேண்டும்.

• **அங்கீகாரம்(Authorisation):** ஒரு வணிகரின் பரிமாற்ற அங்கீகார கோரிக்கைக்கு அட்டை வழங்கும் வங்கியின் பதில், பணம் செலுத்தும் தகவல் செல்லுபடியாகும்தன்மையாகும் , வாடிக்கையாளரின் கடனட்டையில் நிதி உள்ளது என்பதைக் குறிக்கிறது.

• **அட்டைஎண்(Card number):** ஒரு அட்டைக்கு கடனட்டை சங்கம் அல்லது அட்டை வழங்கும் வங்கியால் ஒதுக்கப்பட்ட எண். கடனட்டை மூலம் பணம் செலுத்துவதற்கு இந்தத் தகவல் வாடிக்கையாளர் ஒரு வணிகருக்கு வழங்கப்பட வேண்டும், ஆனால் வேறு யாருடனும் பகிர்ந்து கொள்ளக்கூடாது. இலக்கங்களின் சரம் அட்டையில் அச்சிடப்பட்டுள்ளது.

• **கடனட்டை(Credit card):** ஒரு நிதி நிறுவனத்திடமிருந்து பாதுகாப்பற்ற/ பாதுகாக்கப்பட்ட கடனைப் பெறுவதன் மூலம் பொருட்கள் அல்லது சேவைகளுக்கு பணம் செலுத்த அனுமதிக்கும் அட்டையாகும்.

• **கடன்பெறும் வரம்பு(Credit limit)**: ஒரு நிதி நிறுவனம் வாடிக்கை யாளருக்கு அளிக்கும் அதிகபட்ச கடன் தொகையை இந்த சொல் குறிக்கிறது. கடன் வழங்கும் நிறுவனம், கடன் கோரும் விண்ணப்பதாரரால் கொடுக்கப்பட்ட தகவலின் பகுப்பாய்வு அடிப்படையில் கடனட்டையில் கடன் வரம்பை நீட்டிக்கிறது. கடன்

வரம்பு வாடிக்கையாளரின் கடன்பெறும் மதிப்பெண்கள் எதிர்காலத்தில் கடன் பெறும் திறனைப் பாதிக்கலாம்.

• **(CVV):**இது ஒரு அட்டையின் சரிபார்ப்பு மதிப்பைக் குறிக்கிறது. இது அட்டையில் அச்சிடப்பட்ட மூன்றிலக்க எண்ணாகும் பெரும்பாலான இணைய பரிமாற்றங்களை முடிக்க இது கட்டாயமாகும். இந்த விவரங்கள் இரகசியமானவை யாருடனும் பகிர்ந்துகொள்ளடக்கூடாது.

• **பற்றுஅட்டை(Debit card):** இந்த அட்டையை வைத்திருப்பவரின் வங்கிக் கணக்கில் கிடைக்கும் நிதியைக் கழிப்பதன் மூலம் பொருட்கள் அல்லது சேவைகளுக்கு பணம் செலுத்த அனுமதிக்கும் அட்டையாகும்

• **மின்-வணிக தளம்(E-commerce platform):** இந்த தளம்/இணையதளம் எண்ணிம, மின்னனுவலைபின்னல் மூலம் எண்ணிம உற்பத்திகள் உட்பட பொருட்களை , சேவைகளை வாங்கவும் விற்கவும் உதவுகிறது.

• **(EMI):** இது சமமான மாதாந்திர தவணையைக் குறிக்கிறது. இது ஒரு நிலையான மாதாந்திர கொடுப்பனவு (அசல் , வட்டியை உள்ளடக்கியது) கடனளிப்பவர்/கடனாளிக்கு (வங்கி/NBFC போன்றவை) ஒவ்வொரு மாதமும் கடன் வழங்குபவர்/கடனாளியிடம்

இருந்து பெறப்பட்ட வட்டியுடன் சேர்த்து, கடனாளி/கடன் முடியும் வரை முழுமையாக கடன் வாங்கியவர் செலுத்தும்சமதவணை தொகையாகும்.

• **குறியாக்கம்(Encryption):** செயலாக்கத் தகவலை அதன் இரகசியத்தைப் பேன மின்னணு குறியீடாக மாற்றும் ஒருசெயல்முறையாகும்

. • **காலாவதி தேதி(Expiry date):** ஒரு கடன்/பற்றுஅட்டை, ஒப்பந்தம், உடன்படிக்கை, ஆவணம் போன்றவற்றின் செல்லுபடியாகும் தேதி. இன்னும் காலாவதியாகாத அட்டைகள் அல்லது ஆவணங்கள் தொடர்பாக மட்டுமே பரிமாற்றங்கள் அங்கீகரிக்கப்படும்.

• **நுழைவாயில்(Gateway):** இது ஒரு இடைத்தரகராகும், இது நேரடியாக அதன் ஈடுபாடு இல்லாமல் பரிமாற்றங்களின் அடிப்படை மேலாண்மை, இடர் மேலாண்மை போன்ற சேவைகளை வழிசெலுத்துவதற்கும் செயலாக்குவதற்கும் தொழில்நுட்ப உள்கட்டமைப்பை வழங்குகிறது. பணம் செலுத்தும் நுழைவாயில்கள் என்பது நிதிகளைக் கையாளுவதில் எந்த ஈடுபாடும் இல்லாமல்இணையத்தில் கொடுப்பனவு பரிமாற்றங்களை வழி நடத்துவதற்கும், செயலாக்குவதற்கும் தொழில்நுட்ப உள்கட்டமைப்பை வழங்கும் நிறுவனங்களாகும்.

• **உடனடி கொடுப்பனவுச் சேவைகள் (Immediate payment services (IMPS):)**: இது இந்திய தேசிய கொடுப்பனவு கழகம் (NPCI) வழங்கும் கைபேசிகள் மூலம் உடனடியாக வங்கிகளுக்கு இடையேயான மின்னணு நிதி பரிமாற்ற சேவை (குறிப்பிட்டவரம்பு வரை) ஆகும்.

• **KYC:** இது உங்கள் வாடிக்கையாளரை அறிந்து கொள்ளுங்கள்(Know Your Customer(KYC)) என்பதன் சுருக்கமான பெயராகும் . ஒரு வாடிக்கை யாளருடன் உறவைப் பேணுவதில் உள்ள அடையாளம், பொருத்தம் , அபாயங்கள் ஆகியவற்றைச் சரிபார்க்க நிதி நிறுவனம்இதன்மூலம் ஒரு முயற்சியை மேற்கொள்கிறது.

• **பணக் கழுதை(Money mule):** இது அவர்களின் வங்கிக் கணக்கு(கள்) மூலம் திருடப்பட்ட/சட்டவிரோதமான பணத்தை மோசடி செய்பவர்களால் சுரண்டப்படும் பாதிக்கப்பட்டவர்களை விவரிக்கப் பயன்படும் சொல்லாகும்.

• **பல்லடுக்குநிலைசந்தை(Multi-Level Marketing):** பங்கேற்பாளர்கள் தங்கள் விற்பனை , அவர்கள் ஆட்சேர்ப்பு செய்யும் எந்தவொரு பங்கேற்பாளர் களின் விற்பனையிலும் கழிவுத்தொகையினைப் பெறும் ஒரு அமைப்பில் ஒரு நிறுவனத்தின் சார்பாக பொருட்கள் அல்லது சேவைகளை விற்கும் சங்கிலிதொடர்புபோன்ற நடைமுறையாகும்.

• **தேசிய தானியங்கி தீர்வுஇல்லம் (National Automated Clearing House (NACH)):** இது ஒரு மையப்படுத்தப்பட்ட மின்னனு தீர்வு சேவை (Electronic Clearing Service (ECS)) அமைப்பாகும், இதுஇந்திய தேசிய வழங்கல் நிறுவனத்தின் (National Payments Corporation of India (NPCI).) மூலம் இயக்கப்படுகிறது.

• **அருகாமைபுலத்தொடர்பு (Near Field Communication (NFC)):** இது ஒரு NFC பொருத்தப்பட்ட சாதனத்தில் இருந்து ஒரு திறமையான முனையத்திற்கு தரவை அனுப்ப பயன்படும் ஒரு தகவல் தொடர்பு தொழில்நுட்பமாகும். NFC தொழில்நுட்பம், NFC இயக்கப்பட்ட இயந்திரத்தின் அருகே திறன்பேசியை/அட்டையை வைத்து, தொடர்பு இல்லாத கொடுப்பனவுச் செலுத்தப் பயன்படுகிறது.

• **தேசிய மின்னனு நிதிபரிமாற்றம் (National Electronic Fund Transfer (NEFT)):** இது இந்திய சேமநல வங்கிக்கு(RBI) சொந்தமான இயக்கப்படும் நாடு தழுவிய மையப்படுத்தப்பட்ட நிதிபரிமாற்ற முறையாகும், இது இந்தியாவில் உள்ள வங்கியின் வாடிக்கையாளர்களுக்கு ஏதேனும் இரண்டு NEFT-இயக்கப்பட்ட வங்கிக் கணக்குகளுக்கு இடையே நிதியைப் பரிமாற்றம் செய்ய உதவுகிறது.

• **(OTP):** ஒருமுறை மட்டுமான கடவுச்சொல்(One Time Password(OTP)) என்பது அங்கீகார முறையின் காரணிகளில் ஒன்றாகும், இது

வாடிக்கையாளருக்குத் தெரியும், பெரும்பாலும் இணையத்தில் நிதி பரிமாற்றங்களை மேற்கொள்வதற்குப் பயன்படுத்தப்படுகிறது. இது இரகசியமானது, யாருடனும் பகிர்ந்துகொள்ளக்கூடாது.

• மோசடி**(Phishing):** இது வாடிக்கையாளர்கள் தங்கள் வங்கி / மின்-பணப்பை(E-Wallet) வழங்குநரிடமிருந்து வந்ததாகவும், இரகசிய விவரங்களைப் பிரித்தெடுப் பதற்கான இணைப்புகளைக் கொண்டிருப்பதாகவும் எண்ணிகொண்டு வாடிக்கையாளர்களை ஏமாற்றுவதற்காக வடிவமைக்கப்பட்ட ஏமாற்றப்பட்ட மின்னஞ்சல்கள் /அல்லது குறுஞ்செய்திகளைக் குறிக்கிறது.

• **விற்பணைமுனைம சாதனம் (POS) / ஏற்றுக்கொள்ளும் சாதனம் (mPOS):** இது வணிக நிறுவனங்களில் நிறுவப்பட்ட எந்தவொரு சாதனத்தை / முனைமத்தை / இயந்திரத்தைக் குறிக்கிறது, இது வணிகர்கள் கட்டண அட்டைகள் (கடனட்டைகள், பற்றட்டைகள், பரிசுஅட்டைகள் போன்றவை) மூலம் பணம் செலுத்துவதை அனுமதிக்கின்றது. .

• **விரைவான பதில்செயல்(Quick Response (QR))** குறியீடு: QR குறியீடு என்பது இரு பரிமாண பட்டை குறியீட்டின் ஒருவகையாகும். இது வெள்ளை பின்னணியில் அமைக்கப்பட்ட கருப்பு வண்ணசதுரங்களைக் கொண்டுள்ளது. இந்த குறியீடுகளைப் படிக்கவும் விளக்கமளிக்கவும் திறன்பேசியின் படபிடிப்புக்கள்

போன்ற உருவப்பட சாதனங்களைப் பயன்படுத்தலாம். QR குறியீடு பணம் பெறுபவரைப் பற்றிய தகவல்களைக் கொண்டுள்ளது , வாடிக்கையாளர்களின் கணக்கில் பற்று செய்வதன் மூலம் விற்பனையின் போது கைபேசிகொடுப்பனவுகளை எளிதாக்க பயன்படுகிறது.

• **தொலைநிலை அணுகல்(Remote Access):**வாடிக்கையாளரின் கைபேசியில் / கணினியில் ஒரு பயன்பாட்டைப் பதிவிறக்கம் செய்ய வாடிக்கை யாளரை கவர்ந்திழுப்பதைக் குறிக்கிறது, இதனுடைய உதவியால் அந்த வாடிக்கையாளரின் சாதனத்தில் உள்ள அனைத்து வாடிக்கையாளர்களின் தரவையும் அணுக முடியும்.

• **(UPI):** ஒரேமாதிரியான கொடுப்பனவு இடைமுகம்(Unified Payment Interface) என்பது ஒரு வங்கியின்/ பணப்பையின் கணக்கிலிருந்து மற்றொன்றுக்கு இணைய அணுகல் உள்ள கைபேசியைப் பயன்படுத்தி பணத்தை பரிமாறிகொள்ள அனுமதிக்கும் தளமாகும். ஒரு வாடிக்கையாளர் இந்தUPI க்காக வங்கியில் பதிவு செய்தவுடன், அவருக்கென ஒரு தனிப்பட்ட மெய்நிகர் அடையாளங்காட்டி உருவாக்கப்பட்டு, பணம் செலுத்தத் தொடங்க வாடிக்கையாளரின் கைபேசியில் பதிலிடல்செய்யப்படுகிறது(mapped). இது UPI-PIN வடிவத்தில் அங்கீகாரத்தைப் பயன்படுத்திகொள்கிறது, இது இரகசியமானது இதனை யாருடனும் பகிர்ந்துகொள்ளக்கூடாது.

• **முறைகேடான(Vishing):** இது வங்கி / வங்கி அல்லாத மின்-பணப்பை வழங்குநர் களிடமிருந்து / தொலைத்தொடர்பு சேவை வழங்குநர்களிட மிருந்து வரும் தொலைபேசி அழைப்புகளைக் குறிக்கிறது. ,

• **பணப்பை(Wallet)**: இது ஒரு வங்கிகணக்கு போன்றது அதனால் இதில் சேமிக்கப்பட்ட மதிப்புக்கு எதிராக பொருட்களை சேவைகளை வாங்க பயன்படுத்திகொள்ளலாம். ஒரு பணப்பை மெய்நிகராக (எ.கா. கைபேசி பணப்பை) அல்லது நேரடியாக (முன்கூட்டியேசெலுத்தப்பட்ட அட்டைகளாக) இருக்கலாம்.

FREETAMILEBOOKS.COM

மின்புத்தகங்களைப் படிக்க உதவும் கருவிகள்:

மின்புத்தகங்களைப் படிப்பதற்கென்றே கையிலேயே வைத்துக் கொள்ளக்கூடிய பல கருவிகள் தற்போது சந்தையில் வந்துவிட்டன. Kindle, Nook, Android Tablets போன்றவை இவற்றில் பெரும்பங்கு வகிக்கின்றன. இத்தகைய கருவிகளின் மதிப்பு தற்போது 4000 முதல் 6000 ரூபாய் வரை குறைந்துள்ளன. எனவே பெரும்பான்மையான மக்கள் தற்போது இதனை வாங்கி வருகின்றனர்.

ஆங்கிலத்திலுள்ள மின்புத்தகங்கள்:

ஆங்கிலத்தில் லட்சக்கணக்கான மின்புத்தகங்கள் தற்போது கிடைக்கப் பெறுகின்றன. அவை PDF, EPUB, MOBI, AZW3. போன்ற வடிவங்களில் இருப்பதால், அவற்றை மேற்கூறிய கருவிகளைக் கொண்டு நாம் படித்துவிடலாம்.

தமிழிலுள்ள மின்புத்தகங்கள்:

தமிழில் சமீபத்திய புத்தகங்களெல்லாம் நமக்கு மின்புத்தகங்களாக கிடைக்கப்பெறுவதில்லை. ProjectMadurai.com எனும் குழு தமிழில் மின்புத்தகங்களை வெளியிடுவதற்கான ஓர் உன்னத சேவையில்

ஈடுபட்டுள்ளது. இந்தக் குழு இதுவரை வழங்கியுள்ள தமிழ் மின்புத்தகங்கள் அனைத்தும் PublicDomain-ல் உள்ளன. ஆனால் இவை மிகவும் பழைய புத்தகங்கள்.

சமீபத்திய புத்தகங்கள் ஏதும் இங்கு கிடைக்கப்பெறுவதில்லை.

சமீபத்திய புத்தகங்களை தமிழில் பெறுவது எப்படி?

அமேசான் கிண்டில் கருவியில் தமிழ் ஆதரவு தந்த பிறகு, தமிழ் மின்னூல்கள் அங்கே விற்பனைக்குக் கிடைக்கின்றன. ஆனால் அவற்றை நாம் பதிவிறக்க இயலாது. வேறு யாருக்கும் பகிர இயலாது.

சமீபகாலமாக பல்வேறு எழுத்தாளர்களும், பதிவர்களும், சமீபத்திய நிகழ்வுகளைப் பற்றிய விவரங்களைத் தமிழில் எழுதத் தொடங்கியுள்ளனர். அவை இலக்கியம், விளையாட்டு, கலாச்சாரம், உணவு, சினிமா, அரசியல், புகைப்படக்கலை, வணிகம் மற்றும் தகவல் தொழில்நுட்பம் போன்ற பல்வேறு தலைப்புகளின் கீழ் அமைகின்றன.

நாம் அவற்றையெல்லாம் ஒன்றாகச் சேர்த்து தமிழ் மின்புத்தகங்களை உருவாக்க உள்ளோம்.

அவ்வாறு உருவாக்கப்பட்ட மின்புத்தகங்கள் Creative Commons எனும் உரிமத்தின் கீழ் வெளியிடப்படும். இவ்வாறு வெளியிடுவதன் மூலம் அந்தப் புத்தகத்தை எழுதிய மூல ஆசிரியருக்கான உரிமைகள்

சட்டரீதியாகப் பாதுகாக்கப்படுகின்றன. அதே நேரத்தில் அந்த மின்புத்தகங்களை யார் வேண்டுமானாலும், யாருக்கு வேண்டுமானாலும், இலவசமாக வழங்கலாம்.

எனவே தமிழ் படிக்கும் வாசகர்கள் ஆயிரக்கணக்கில் சமீபத்திய தமிழ் மின்புத்தகங்களை இலவசமாகவே பெற்றுக் கொள்ள முடியும்.

தமிழிலிருக்கும் எந்த வலைப்பதிவிலிருந்து வேண்டுமானாலும் பதிவுகளை எடுக்கலாமா?

கூடாது.

ஒவ்வொரு வலைப்பதிவும் அதற்கென்றே ஒருசில அனுமதிகளைப் பெற்றிருக்கும். ஒரு வலைப்பதிவின் ஆசிரியர் அவரது பதிப்புகளை "யார் வேண்டுமானாலும் பயன்படுத்தலாம்" என்று குறிப்பிட்டிருந்தால் மட்டுமே அதனை நாம் பயன்படுத்த முடியும்.

அதாவது "Creative Commons" எனும் உரிமத்தின் கீழ் வரும் பதிப்புகளை மட்டுமே நாம் பயன்படுத்த முடியும்.

அப்படி இல்லாமல் "All Rights Reserved" எனும் உரிமத்தின் கீழ் இருக்கும் பதிப்புகளை நம்மால் பயன்படுத்த முடியாது.

வேண்டுமானால் "All Rights Reserved" என்று விளங்கும் வலைப்பதிவுகளைக் கொண்டிருக்கும் ஆசிரியருக்கு அவரது

பதிப்புகளை “Creative Commons” உரிமத்தின் கீழ் வெளியிடக்கோரி நாம் நமது வேண்டுகோளைத் தெரிவிக்கலாம். மேலும் அவரது படைப்புகள் அனைத்தும் அவருடைய பெயரின் கீழே தான் வெளியிடப்படும் எனும் உறுதியையும் நாம் அளிக்க வேண்டும்.

பொதுவாக புதுப்புது பதிவுகளை உருவாக்குவோருக்கு அவர்களது பதிவுகள் நிறைய வாசகர்களைச் சென்றடைய வேண்டும் என்ற எண்ணம் இருக்கும். நாம் அவர்களது படைப்புகளை எடுத்து இலவச மின்புத்தகங்களாக வழங்குவதற்கு நமக்கு அவர்கள் அனுமதியளித்தால், உண்மையாகவே அவர்களது படைப்புகள் பெரும்பான்மையான மக்களைச் சென்றடையும். வாசகர்களுக்கும் நிறைய புத்தகங்கள் படிப்பதற்குக் கிடைக்கும்

வாசகர்கள் ஆசிரியர்களின் வலைப்பதிவு முகவரிகளில் கூட அவர்களுடைய படைப்புகளை தேடிக் கண்டுபிடித்து படிக்கலாம். ஆனால் நாங்கள் வாசகர்களின் சிரமத்தைக் குறைக்கும் வண்ணம் ஆசிரியர்களின் சிதறிய வலைப்பதிவுகளை ஒன்றாக இணைத்து ஒரு முழு மின்புத்தகங்களாக உருவாக்கும் வேலையைச் செய்கிறோம். மேலும் அவ்வாறு உருவாக்கப்பட்ட புத்தகங்களை “மின்புத்தகங்களைப் படிக்க உதவும் கருவிகள்”-க்கு ஏற்ற வண்ணம் வடிவமைக்கும் வேலையையும் செய்கிறோம்.

FREETAMILEBOOKS.COM

இந்த வலைத்தளத்தில்தான் பின்வரும் வடிவமைப்பில் மின்புத்தகங்கள் காணப்படும்.

PDF for desktop, PDF for 6” devices, EPUB, AZW3, ODT

இந்த வலைதளத்திலிருந்து யார் வேண்டுமானாலும் மின்புத்தகங்களை இலவசமாகப் பதிவிறக்கம்(download) செய்து கொள்ளலாம்.

அவ்வாறு பதிவிறக்கம்(download) செய்யப்பட்ட புத்தகங்களை யாருக்கு வேண்டுமானாலும் இலவசமாக வழங்கலாம்.

இதில் நீங்கள் பங்களிக்க விரும்புகிறீர்களா?

நீங்கள் செய்யவேண்டியதெல்லாம் தமிழில் எழுதப்பட்டிருக்கும் வலைப்பதிவுகளிலிருந்து பதிவுகளை
எடுத்து, அவற்றை LibreOffice/MS Office போன்ற wordprocessor-ல் போட்டு ஓர் எளிய மின்புத்தகமாக மாற்றி எங்களுக்கு அனுப்பவும்.

அவ்வளவுதான்!

மேலும் சில பங்களிப்புகள் பின்வருமாறு:

1. ஒருசில பதிவர்கள்/எழுத்தாளர்களுக்கு அவர்களது படைப்புகளை “Creative Commons” உரிமத்தின்கீழ் வெளியிடக்கோரி மின்னஞ்சல் அனுப்புதல்

2. தன்னார்வலர்களால் அனுப்பப்பட்ட மின்புத்தகங்களின் உரிமைகளையும் தரத்தையும் பரிசோதித்தல்
3. சோதனைகள் முடிந்து அனுமதி வழங்கப்பட்ட தரமான மின்புத்தகங்களை நமது வலைதளத்தில் பதிவேற்றம் செய்தல்

விருப்பமுள்ளவர்கள் freetamilebooksteam@gmail.com எனும் முகவரிக்கு மின்னஞ்சல் அனுப்பவும்.

இந்தத் திட்டத்தின் மூலம் பணம் சம்பாதிப்பவர்கள் யார்?

யாருமில்லை.

இந்த வலைத்தளம் முழுக்க முழுக்க தன்னார்வலர்களால் செயல்படுகின்ற ஒரு வலைத்தளம் ஆகும். இதன் ஒரே நோக்கம் என்னவெனில் தமிழில் நிறைய மின்புத்தகங்களை உருவாக்குவதும், அவற்றை இலவசமாக பயனர்களுக்கு வழங்குவதுமே ஆகும்.

மேலும் இவ்வாறு உருவாக்கப்பட்ட மின்புத்தகங்கள், ebook reader ஏற்றுக்கொள்ளும் வடிவமைப்பில் அமையும்.

இத்திட்டத்தால் பதிப்புகளை எழுதிக்கொடுக்கும் ஆசிரியர்/பதிவருக்கு என்ன லாபம்?

ஆசிரியர்/பதிவர்கள் இத்திட்டத்தின் மூலம் எந்தவிதமான தொகையும் பெறப்போவதில்லை. ஏனெனில், அவர்கள் புதிதாக இதற்கென்று எந்தஒரு பதிவையும் எழுதித்தரப்போவதில்லை.

ஏற்கனவே அவர்கள் எழுதி வெளியிட்டிருக்கும் பதிவுகளை எடுத்துத்தான் நாம் மின்புத்தகமாக வெளியிடப்போகிறோம்.

அதாவது அவரவர்களின் வலைதளத்தில் இந்தப் பதிவுகள் அனைத்தும் இலவசமாகவே கிடைக்கப்பெற்றாலும், அவற்றையெல்லாம் ஒன்றாகத் தொகுத்து ebook reader போன்ற கருவிகளில் படிக்கும் விதத்தில் மாற்றித் தரும் வேலையை இந்தத் திட்டம் செய்கிறது.

தற்போது மக்கள் பெரிய அளவில் tablets மற்றும் ebook readers போன்ற கருவிகளை நாடிச் செல்வதால் அவர்களை நெருங்குவதற்கு இது ஒரு நல்ல வாய்ப்பாக அமையும்.

நகல் எடுப்பதை அனுமதிக்கும் வலைதளங்கள் ஏதேனும் தமிழில் உள்ளதா?

உள்ளது.

பின்வரும் தமிழில் உள்ள வலைதளங்கள் நகல் எடுப்பதினை அனுமதிக்கின்றன.

1. http://www.vinavu.com
2. http://www.badriseshadri.in
3. http://maattru.com
4. http://www.kaniyam.com
5. http://blog.ravidreams.net

எவ்வாறு ஓர் எழுத்தாளரிடம் CREATIVE COMMONS உரிமத்தின் கீழ் அவரது படைப்புகளை வெளியிடுமாறு கூறுவது?

இதற்கு பின்வருமாறு ஒரு மின்னஞ்சலை அனுப்ப வேண்டும்.

துவக்கம்

உங்களது வலைத்தளம் அருமை (வலைதளத்தின் பெயர்).

தற்போது படிப்பதற்கு உபயோகப்படும் கருவிகளாக Mobiles மற்றும் பல்வேறு கையிருப்புக் கருவிகளின் எண்ணிக்கை அதிகரித்து வந்துள்ளது.

இந்நிலையில் நாங்கள் http://www.FreeTamilEbooks.com எனும் வலைதளத்தில், பல்வேறு தமிழ் மின்புத்தகங்களை வெவ்வேறு துறைகளின் கீழ் சேகரிப்பதற்கான ஒரு புதிய திட்டத்தில் ஈடுபட்டுள்ளோம்.

இங்கு சேகரிக்கப்படும் மின்புத்தகங்கள் பல்வேறு கணிணிக் கருவிகளான Desktop,ebook readers like kindl, nook, mobiles, tablets with android, iOS போன்றவற்றில் படிக்கும் வண்ணம் அமையும். அதாவது இத்தகைய கருவிகள் support செய்யும் odt, pdf, ebub, azw போன்ற வடிவமைப்பில் புத்தகங்கள் அமையும்.

இதற்காக நாங்கள் உங்களது வலைதளத்திலிருந்து பதிவுகளை பெற விரும்புகிறோம். இதன் மூலம் உங்களது பதிவுகள் உலகளவில் இருக்கும் வாசகர்களின் கருவிகளை நேரடியாகச் சென்றடையும்.

எனவே உங்களது வலைதளத்திலிருந்து பதிவுகளை பிரதியெடுப்பதற்கும் அவற்றை மின்புத்தகங்களாக மாற்றுவதற்கும் உங்களது அனுமதியை வேண்டுகிறோம்.

இவ்வாறு உருவாக்கப்பட்ட மின்புத்தகங்களில் கண்டிப்பாக ஆசிரியராக உங்களின் பெயரும் மற்றும் உங்களது வலைதள முகவரியும் இடம்பெறும். மேலும் இவை “Creative Commons” உரிமத்தின் கீழ் மட்டும்தான் வெளியிடப்படும் எனும் உறுதியையும் அளிக்கிறோம்.

http://creativecommons.org/licenses/

நீங்கள் எங்களை பின்வரும் முகவரிகளில் தொடர்பு கொள்ளலாம்.

e-mail : FREETAMILEBOOKSTEAM@GMAIL.COM
FB : https://www.facebook.com/FreeTamilEbooks

G plus: https://plus.google.com/communities/108817760492177970948

நன்றி.

முடிவு

மேற்கூறியவாறு ஒரு மின்னஞ்சலை உங்களுக்குத் தெரிந்த அனைத்து எழுத்தாளர்களுக்கும் அனுப்பி அவர்களிடமிருந்து அனுமதியைப் பெறுங்கள்.

முடிந்தால் அவர்களையும் “Creative Commons License”-ஐ அவர்களுடைய வலைதளத்தில் பயன்படுத்தச் சொல்லுங்கள்.

கடைசியாக அவர்கள் உங்களுக்கு அனுமதி அளித்து அனுப்பியிருக்கும் மின்னஞ்சலைFREETAMILEBOOKSTEAM@GMAIL.COM எனும் முகவரிக்கு அனுப்பி வையுங்கள்.

ஓர் எழுத்தாளர் உங்களது உங்களது வேண்டுகோளை மறுக்கும் பட்சத்தில் என்ன செய்வது?

அவர்களையும் அவர்களது படைப்புகளையும் அப்படியே விட்டுவிட வேண்டும்.

ஒருசிலருக்கு அவர்களுடைய சொந்த முயற்சியில் மின்புத்தகம் தயாரிக்கும் எண்ணம்கூட இருக்கும். ஆகவே அவர்களை நாம் மீண்டும் மீண்டும் தொந்தரவு செய்யக் கூடாது.

அவர்களை அப்படியே விட்டுவிட்டு அடுத்தடுத்த எழுத்தாளர்களை நோக்கி நமது முயற்சியைத் தொடர வேண்டும்.

மின்புத்தகங்கள் எவ்வாறு அமைய வேண்டும்?

ஒவ்வொருவரது வலைத்தளத்திலும் குறைந்தபட்சம் நூற்றுக்கணக்கில் பதிவுகள் காணப்படும். அவை வகைப்படுத்தப்பட்டோ அல்லது வகைப்படுத்தப் படாமலோ இருக்கும்.

நாம் அவற்றையெல்லாம் ஒன்றாகத் திரட்டி ஒரு பொதுவான தலைப்பின்கீழ் வகைப்படுத்தி மின்புத்தகங்களாகத் தயாரிக்கலாம். அவ்வாறு வகைப்படுத்தப்படும் மின்புத்தகங்களை பகுதி-I பகுதி-II என்றும் கூட தனித்தனியே பிரித்துக் கொடுக்கலாம்.

தவிர்க்க வேண்டியவைகள் யாவை?

இனம், பாலியல் மற்றும் வன்முறை போன்றவற்றைத் தூண்டும் வகையான பதிவுகள் தவிர்க்கப்பட வேண்டும்.

எங்களைத் தொடர்பு கொள்வது எப்படி?

நீங்கள் பின்வரும் முகவரிகளில் எங்களைத் தொடர்பு கொள்ளலாம்.

- EMAIL : FREETAMILEBOOKSTEAM@GMAIL.COM
- Facebook: https://www.facebook.com/FreeTamilEbooks
- Google Plus: https://plus.google.com/communities/108817760492177970948

இத்திட்டத்தில் ஈடுபட்டுள்ளவர்கள் யார்?

குழு – http://freetamilebooks.com/meet-the-team/

SUPPORTED BY

கணியம் அறக்கட்டளை http://kaniyam.com/foundation

கணியம் அறக்கட்டளை

தொலை நோக்கு – Vision

தமிழ் மொழி மற்றும் இனக்குழுக்கள் சார்ந்த மெய்நிகர்வளங்கள், கருவிகள் மற்றும் அறிவுத்தொகுதிகள், அனைவருக்கும் கட்டற்ற அணுக்கத்தில் கிடைக்கும் சூழல்

பணி இலக்கு – Mission

அறிவியல் மற்றும் சமூகப் பொருளாதார வளர்ச்சிக்கு ஒப்ப, தமிழ் மொழியின் பயன்பாடு வளர்வதை உறுதிப்படுத்துவதும், அனைத்து அறிவுத் தொகுதிகளும், வளங்களும் கட்டற்ற அணுக்கத்தில் அனைவருக்கும் கிடைக்கச்செய்தலும்.

தற்போதைய செயல்கள்

- கணியம் மின்னிதழ் – http://kaniyam.com
- கிரியேட்டிவ் காமன்சு உரிமையில் இலவச தமிழ் மின்னூல்கள் – http://FreeTamilEbooks.com

கட்டற்ற மென்பொருட்கள்

- உரை ஒலி மாற்றி – Text to Speech
- எழுத்துணரி – Optical Character Recognition
- விக்கிமூலத்துக்கான எழுத்துணரி
- மின்னூல்கள் கிண்டில் கருவிக்கு அனுப்புதல் – Send2Kindle
- விக்கிப்பீடியாவிற்கான சிறு கருவிகள்
- மின்னூல்கள் உருவாக்கும் கருவி
- உரை ஒலி மாற்றி – இணைய செயலி
- சங்க இலக்கியம் – ஆன்டிராய்டு செயலி
- FreeTamilEbooks – ஆன்டிராய்டு செயலி

- FreeTamilEbooks – ஐஓஎஸ் செயலி
- WikisourceEbooksReportஇந்திய மொழிகளுக்ககான விக்கிமூலம் மின்னூல்கள் பதிவிறக்கப் பட்டியல்
- FreeTamilEbooks.com – Download counter மின்னூல்கள் பதிவிறக்கப் பட்டியல்

அடுத்த திட்டங்கள்/மென்பொருட்கள்

- விக்கி மூலத்தில் உள்ள மின்னூல்களை பகுதிநேர/முழு நேரப் பணியாளர்கள் மூலம் விரைந்து பிழை திருத்துதல்
- முழு நேர நிரலரை பணியமர்த்தி பல்வேறு கட்டற்ற மென்பொருட்கள் உருவாக்குதல்
- தமிழ் NLP க்கான பயிற்சிப் பட்டறைகள் நடத்துதல்
- கணியம் வாசகர் வட்டம் உருவாக்குதல்
- கட்டற்ற மென்பொருட்கள், கிரியேட்டிவ் காமன்சு உரிமையில் வளங்களை உருவாக்குபவர்களைக் கண்டறிந்து ஊக்குவித்தல்

- கணியம் இதழில் அதிக பங்களிப்பாளர்களை உருவாக்குதல், பயிற்சி அளித்தல்
- மின்னூலாக்கத்துக்கு ஒரு இணையதள செயலி
- எழுத்துணரிக்கு ஒரு இணையதள செயலி
- தமிழ் ஒலியோடைகள் உருவாக்கி வெளியிடுதல்
- http://OpenStreetMap.org ல் உள்ள இடம், தெரு, ஊர் பெயர்களை தமிழாக்கம் செய்தல்
- தமிழ்நாடு முழுவதையும் http://OpenStreetMap.org ல் வரைதல்
- குழந்தைக் கதைகளை ஒலி வடிவில் வழங்குதல்
- http://Ta.wiktionary.org ஐ ஒழுங்குபடுத்தி API க்கு தோதாக மாற்றுதல்
- http://Ta.wiktionary.org க்காக ஒலிப்பதிவு செய்யும் செயலி உருவாக்குதல்
- தமிழ் எழுத்துப் பிழைத்திருத்தி உருவாக்குதல்
- தமிழ் வேர்ச்சொல் காணும் கருவி உருவாக்குதல்

- எல்லா http://FreeTamilEbooks.com மின்னூல்களையும் Google Play Books, GoodReads.com ல் ஏற்றுதல்
- தமிழ் தட்டச்சு கற்க இணைய செயலி உருவாக்குதல்
- தமிழ் எழுதவும் படிக்கவும் கற்ற இணைய செயலி உருவாக்குதல் (aamozish.com/Course_preface போல)

மேற்கண்ட திட்டங்கள், மென்பொருட்களை உருவாக்கி செயல்படுத்த உங்கள் அனைவரின் ஆதரவும் தேவை. உங்களால் எவ்வாறேனும் பங்களிக்க இயலும் எனில் உங்கள் விவரங்களை kaniyamfoundation@gmail.com க்கு மின்னஞ்சல் அனுப்புங்கள்.

வெளிப்படைத்தன்மை

கணியம் அறக்கட்டளையின் செயல்கள், திட்டங்கள், மென்பொருட்கள் யாவும் அனைவருக்கும் பொதுவானதாகவும், 100% வெளிப்படைத்தன்மையுடனும் இருக்கும்.இந்த இணைப்பில் செயல்களையும், இந்த இணைப்பில் மாத அறிக்கை, வரவு செலவு விவரங்களுடனும் காணலாம்.

கணியம் அறக்கட்டளையில் உருவாக்கப்படும் மென்பொருட்கள் யாவும் கட்டற்ற மென்பொருட்களாக மூல நிரலுடன், GNU GPL, Apache, BSD, MIT, Mozilla ஆகிய உரிமைகளில் ஒன்றாக வெளியிடப்படும். உருவாக்கப்படும் பிற வளங்கள், புகைப்படங்கள், ஒலிக்கோப்புகள், காணொளிகள், மின்னூல்கள், கட்டுரைகள் யாவும் யாவரும் பகிரும், பயன்படுத்தும் வகையில் கிரியேட்டிவ் காமன்சு உரிமையில் இருக்கும்.

நன்கொடை

உங்கள் நன்கொடைகள் தமிழுக்கான கட்டற்ற வளங்களை உருவாக்கும் செயல்களை சிறந்த வகையில் விரைந்து செய்ய ஊக்குவிக்கும்.

பின்வரும் வங்கிக் கணக்கில் உங்கள் நன்கொடைகளை அனுப்பி, உடனே விவரங்களை kaniyamfoundation@gmail.com க்கு மின்னஞ்சல் அனுப்புங்கள்.

Kaniyam Foundation
Account Number : 606 1010 100 502 79
Union Bank Of India
West Tambaram, Chennai
IFSC – UBIN0560618
Account Type : Current Account

UPI செயலிகளுக்கான QR Code

BHIM UPI Payments Accepted at

Kaniyam Foundation

Account Number : 606101010050279, IFSC Code: UBIN0560618

Scan and Pay using any UPI supported Apps

குறிப்பு: சில UPI செயலிகளில் இந்த QR Code வேலை செய்யாமல் போகலாம். அச்சமயம் மேலே உள்ள வங்கிக் கணக்கு எண், IFSC code ஐ பயன்படுத்தவும்.

Note: Sometimes UPI does not work properly, in that case kindly use Account number and IFSC code for internet banking.